

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-276457

(43)Date of publication of application : 06.10.2000

(51)Int.Cl. G06F 15/177
G06F 13/00
H04L 12/54
H04L 12/58

(21)Application number : 11-081049

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 25.03.1999

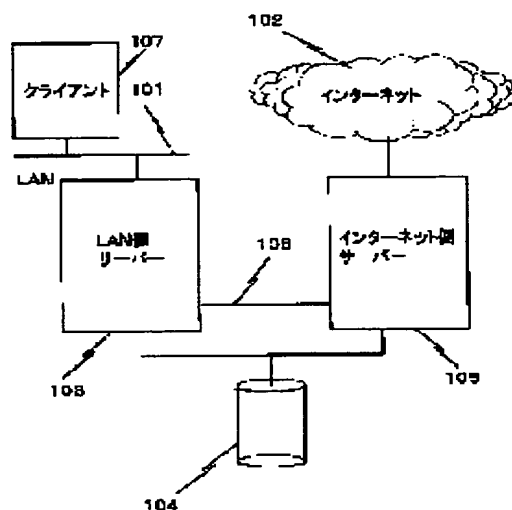
(72)Inventor : SAKAKURA TAKASHI

(54) DATA SHARING COMPUTER SYSTEM AND CLIENT

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain a service copy server which safely shares data between different networks like an intra-enterprise network and the Internet and which copies services for each network.

SOLUTION: A LAN-side server 103 connected to a LAN 101 and an Ininternet-side server 105 connected to the Internet 102 share data on a shared disk 104 for which they use a bus 106 with a bus lock function to exclusively control, and they use this data to provide the same services respectively.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

11-5-57

Dear Mr. [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

5

[illegible]

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2000-276457

(P 2000-276457A)

(43) 公開日 平成12年10月6日 (2000. 10. 6)

(51) Int. Cl. ⁷

識別記号

F I

テーマコード* (参考)

G 0 6 F 15/177

6 8 2

G 0 6 F 15/177

6 8 2

F 5B045

13/00

3 5 1

13/00

3 5 1

Z 5B089

H 0 4 L 12/54

H 0 4 L 11/20

1 0 1

A 5K030

12/58

審査請求 未請求 請求項の数 1 1 O L

(全 2 6 頁)

(21) 出願番号

特願平11-81049

(22) 出願日

平成11年3月25日 (1999. 3. 25)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 坂倉 隆史

東京都千代田区丸の内二丁目2番3号 三菱
電機株式会 社内

(74) 代理人 100102439

弁理士 宮田 金雄 (外2名)

F ターム (参考) 5B045 BB12 EE06 GG01 JJ33

5B089 GA11 GA19 GA21 HA06 HA08

HA10 KA00 KA17 KB13 KC28

KC57 KC58 KD02 KH30

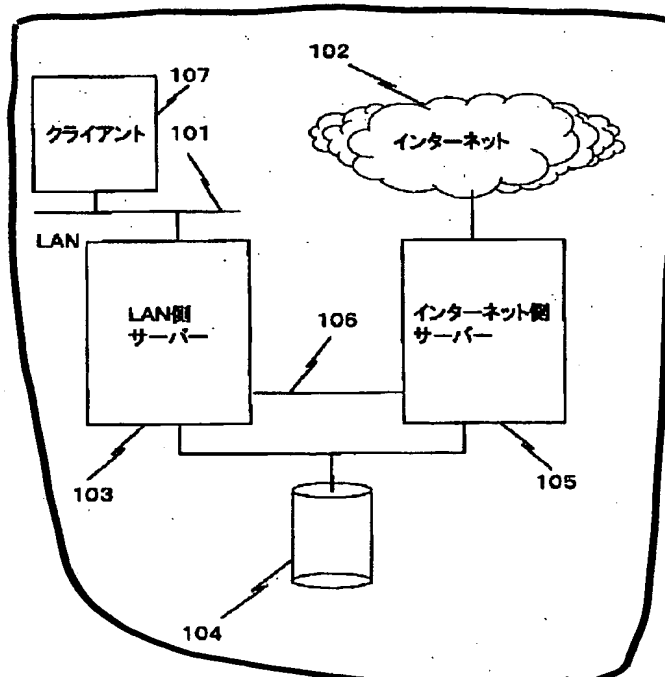
5K030 GA15 HC01 HC13 HD06 KA02

(54) 【発明の名称】 データ共有コンピュータシステム及びクライアント

(57) 【要約】

【課題】 企業内ネットワークとインターネットのように異なるネットワーク間で安全にデータを共有し、ネットワーク毎にサービスを複製するサービス複製サーバーを提供する。

【解決手段】 LAN 101 に接続された LAN 側サーバー 103 と、インターネット 102 に接続されたインターネット側サーバー 105 とが、バスロック機能付きバス 106 を用いて排他制御する共有ディスク 104 上でデータを共有し、そのデータを用いて、それぞれに同一のサービスを提供することを特徴とする。



【特許請求の範囲】

【請求項1】 第一のコンピュータシステムと、第二のコンピュータシステムと、共有データ記憶部と、アクセス可否情報記憶部とを備えるデータ共有コンピュータシステムであって、(A) 共有データ記憶部は、複数のデータ記憶領域を有し、第一のコンピュータシステム及び第二のコンピュータシステムからアクセスされる共有データを、複数のデータ記憶領域に分割して記憶し、

(B) アクセス可否情報記憶部は、共有データ記憶部の各データ記憶領域に対応して、そのデータ記憶領域に対してアクセス可能あるいはアクセス不可であることを意味するアクセス可否情報を記憶し、(C) 第一のコンピュータシステムは、第一のサービス部と、共有データ記憶部に接続する第一のデータアクセス部と、アクセス可否情報記憶部に接続する第一の排他制御部とを備え、

(1) 第一のサービス部は、第一のデータアクセス部と第一の排他制御部に対して、任意のデータ記憶領域に対するアクセスを指示し、

(2) 第一の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更し、

(3) 第一のデータアクセス部は、第一の排他制御部により、アクセス可能と判定され、アクセス可否情報をアクセス不可に変更された後に、指示されたデータ記憶領域にアクセスし、

(4) 第一の排他制御部は、第一のデータアクセス部により、指示されたデータ記憶領域に対してアクセスされた後に、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス可能に変更し、(D) 第二のコンピュータシステムは、第二のサービス部と、共有データ記憶部に接続する第二のデータアクセス部と、アクセス可否情報記憶部に接続する第二の排他制御部とを備え、

(1) 第二のサービス部は、第二のデータアクセス部と第二の排他制御部に対して、任意のデータ記憶領域に対するアクセスを指示し、

(2) 第二の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更し、

(3) 第二のデータアクセス部は、第二の排他制御部により、アクセス可能と判定され、アクセス可否情報をアクセス不可に変更された後に、指示されたデータ記憶領域にアクセスし、

(4) 第二の排他制御部は、第二のデータアクセス部により、指示されたデータ記憶領域に対してアクセスされた後に、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス可能に変更することを特徴とするデ

ータ共有コンピュータシステム。

【請求項2】 第一のコンピュータシステムは、第三のコンピュータシステムを有する第一のネットワークシステムに接続し、

第一のサービス部は、第一のネットワークシステムを介して第三のコンピュータシステムに対してサービスを提供し、

第二のコンピュータシステムは、第四のコンピュータシステムを有する第二のネットワークシステムに接続し、

10 第二のサービス部は、第二のネットワークシステムを介して第四のコンピュータシステムに対してサービスを提供することを特徴とする請求項1記載のデータ共有コンピュータシステム。

【請求項3】 第二のサービス部は、第一のサービス部が第一のネットワークシステムを介して第三のコンピュータシステムに対して提供するサービスと等価のサービスを、第二のネットワークシステムを介して第四のコンピュータシステムに対して提供することを特徴とする請求項2記載のデータ共有コンピュータシステム。

20 【請求項4】 第一の排他制御部は、バスロック機能付きバスによって、アクセス可否情報記憶部に接続し、第一の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更する間、バスをロックし、

30 第一の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス可能に変更する間、バスをロックし、

第二の排他制御部は、上記バスロック機能付きバスによって、アクセス可否情報記憶部に接続し、

第二の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更する間、バスをロックし、

40 第二の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス可能に変更する間、バスをロックすることを特徴とする請求項1記載のデータ共有コンピュータシステム。

【請求項5】 第一の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更する一連の動作を、一の命令で実行し、

50 第二の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶

領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更する一連の動作を、一の命令で実行すること特徴とする請求項1記載のデータ共有コンピュータシステム。

【請求項6】 第一のコンピュータシステムは、以下の要素を備えることを特徴とする請求項1記載のデータ共有コンピュータシステム

(1) データの暗号化及び復号化に用いる暗号鍵を記憶する暗号鍵記憶部、(2) 暗号鍵を指定して暗号化を指示された場合には、指定された暗号鍵を用いてデータを暗号化し、暗号鍵を指定して復号化を指示された場合には、指定された暗号鍵を用いてデータを復号化するデータ暗号化／復号化実行部、(3) 暗号鍵記憶部が記憶する暗号鍵を変更する暗号鍵再設定部、(4) 第一のデータアクセス部に、データ記憶領域からの暗号データの読み出しを指示し、データ暗号化／復号化実行部に、変更前の暗号鍵を指定して、読み出した暗号データの復号化を指示し、データ暗号化／復号化実行部に、変更後の暗号鍵を指定して、復号化したデータの再暗号化を指示し、第一のデータアクセス部に、再暗号化したデータを、元のデータ記憶領域へ書き込むことを指示するデータ再暗号化部。

【請求項7】 ネットワークシステムに接続するクライアントであって、以下の要素を有するクライアント

(1) 上記ネットワークシステムに接続する第一のコンピュータシステムであって、第二のコンピュータシステムとデータを共有する第一のコンピュータシステムに対して、共有データを送信し、また、共有データを受信する共有データ送信／受信部、(2) データ送信／受信部が送信する共有データを暗号化するデータ暗号化部、(3) データ送信／受信部が受信した共有データを復号化するデータ復号化部。

【請求項8】 データ共有コンピュータシステムは、第三のコンピュータシステムを有し、第三のコンピュータシステムは、第一のコンピュータシステムが接続する第一のネットワークシステムに接続し、第一のサービス部は、第一のネットワークシステムを介して第三のコンピュータシステムに対してサービスを提供し、第三のコンピュータシステムは、第一のサービス部が提供するサービスによってアクセスした共有データをキャッシュする共有データキャッシュ部を有することを特徴とする請求項1記載のデータ共有コンピュータシステム。

【請求項9】 第一のサービス部は、第一の構成情報を用いて動作し、共有データ記憶部は、第一のサービス部が用いる第一の

構成情報を記憶し、

第二のコンピュータシステムは、他の記憶部を有し、第二のコンピュータシステムは、共有データ記憶部に記憶されている第一の構成情報を読み出し、読み込んだ第一の構成情報を他の記憶部に書き込む構成情報複製部を有し、

第二のサービス部は、他の記憶部に書き込んだ第一の構成情報を更新し、更新した第二の構成情報を用いて動作することを特徴とする請求項1記載のデータ共有コンピュータシステム。

【請求項10】 第一のコンピュータシステムは、以下の要素を備えることを特徴とする請求項1記載のデータ共有コンピュータシステム

(1) 第一のコンピュータシステムによるユーザ認証の認証方式を記憶する認証方式管理部と、(2) 認証に用いるデータを予め記憶する認証データベース管理部と、

(3) 認証要求と認証を受ける為のデータとを受付け、認証を受ける為のデータと、認証データベース管理部に予め記憶された認証に用いるデータとを用いて、認証方式管理部に記憶された認証方式により、ユーザ認証を行なう認証機能部。

【請求項11】 データ共有コンピュータシステムは、バスを備え、第一のコンピュータシステムと、第二のコンピュータシステムと、共有データ記憶部と、アクセス可否情報記憶部とが上記バスに接続された共有メモリ型並列計算機であることを特徴とする請求項1記載のデータ共有コンピュータシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、第三者がアクセスし、利用するインターネットなどのネットワーク上で、安全にデータ提供サービスを行なうサーバー装置に係り、第三者のアクセスから保護すべきネットワークとデータを共有するサーバー装置に関する。

【0002】

【従来の技術】 近年インターネット利用が普及し、WWW (World Wide Web)、電子メールなどのインターネットを利用したアプリケーションの利用がごく一般的に行なわれるようになってきた。これらのアプリケーションによって、インターネットを利用して、企業や、教育機関などが提供する情報を参照することや、通信目的の利用が可能になった。

【0003】 しかし、インターネットに接続することは、インターネット上に接続されたいずれのサイトにも自由にアクセスできるという利便性をもたらす一方、悪意の第三者からの攻撃に晒されるという危険性をもたらすことを意味する。

【0004】 そこで、一般に企業では、企業内のネットワークシステムをインターネット接続する必要がある場合、インターネットへの接続箇所を限定し、その個所に

10

20

30

40

50

ファイアウォールと呼ばれる、特定の通信のみその通過を許す機構を設け、そのファイアウォールを介して接続することにより、企業内のネットワークをインターネット経由の第三者からの攻撃から保護する運用がなされてきた。そして、一般に企業内ネットワークの安全性がインターネット接続の利便性より重視されるため、ファイアウォールの構成としては、ごく限られた通信、例えば、電子メールの送信プロトコルである SMTP (simple mail transfer protocol) メッセージのみが通過できるというものが多い。

【0005】これに対して、特開平9-270788には、ファイアウォールの運用において、インターネット接続の利便性と安全性を両立させるために、通信パケットにファイアウォールからの認証チャレンジにตอบสนองするプログラム機能を持たせ、特定の認証ポートを通して通信できるようにすることにより、ファイアウォールの構成を変えなくてもインターネットからの種々のサービス要求に対応できる技術が開示されている。これにより、企業内のネットワークの安全を保証しながら、ネットワークへのアクセスを認められた特定のユーザーに、より柔軟なサービスを企業内のネットワークから提供することができる。

【0006】しかし、企業内のネットワークとインターネットを接続して利用する場合に、上述の技術を利用しても依然として企業内ネットワークとインターネットで安全にデータを共有をすることは難しい。

【0007】なお、インターネットを安価な通信媒体として利用する場合には、通信経路からのデータ漏洩から守るために、送信データを暗号化して送信することが行なわれているが、このようなデータの暗号／復号化は、システムのいろいろなレベルで行なわれている。例えば、通信ソケットレベルで行なわれる暗号化サービスとしてSSL (secure sockets layer) が知られており、また、特開平9-251426のようにファイルシステムというアプリケーションレベルでデータの暗号／復号化する技術が知られている。

【0008】

【発明が解決しようとする課題】本発明は、上記した従来技術の欠点を除くためになされたものであって、その目的とするところは、安全に企業内ネットワークとインターネットでデータ共有を実現するデータ共有機構と、共有データを利用するアプリケーションの管理方法及び装置を提供することである。つまり、本発明は、企業内ネットワークあるいはインターネットのいずれからも、共有データにアクセス可能な構成と、企業内ネットワーク内のアプリケーションとインターネット上のアプリケーションが、アプリケーションの管理方法によって共有データを参照／更新して、等価なサービスを各々のネットワークに対して与える構成とを提供することを課題とする。

【0009】

【課題を解決するための手段】この発明に係るデータ共有コンピュータシステムは、第一のコンピュータシステムと、第二のコンピュータシステムと、共有データ記憶部と、アクセス可否情報記憶部とを備えるデータ共有コンピュータシステムであって、(A)共有データ記憶部は、複数のデータ記憶領域を有し、第一のコンピュータシステム及び第二のコンピュータシステムからアクセスされる共有データを、複数のデータ記憶領域に分割して記憶し、(B)アクセス可否情報記憶部は、共有データ記憶部の各データ記憶領域に対応して、そのデータ記憶領域に対してアクセス可能あるいはアクセス不可であることを意味するアクセス可否情報を記憶し、(C)第一のコンピュータシステムは、第一のサービス部と、共有データ記憶部に接続する第一のデータアクセス部と、アクセス可否情報記憶部に接続する第一の排他制御部とを備え、(1)第一のサービス部は、第一のデータアクセス部と第一の排他制御部に対して、任意のデータ記憶領域に対するアクセスを指示し、(2)第一の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更し、(3)第一のデータアクセス部は、第一の排他制御部により、アクセス可能と判定され、アクセス可否情報をアクセス不可に変更された後に、指示されたデータ記憶領域にアクセスし、(4)第一の排他制御部は、第一のデータアクセス部により、指示されたデータ記憶領域に対してアクセスされた後に、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス可能に変更し、(D)第二のコンピュータシステムは、第二のサービス部と、共有データ記憶部に接続する第二のデータアクセス部と、アクセス可否情報記憶部に接続する第二の排他制御部とを備え、(1)第二のサービス部は、第二のデータアクセス部と第二の排他制御部に対して、任意のデータ記憶領域に対するアクセスを指示し、(2)第二の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更し、(3)第二のデータアクセス部は、第二の排他制御部により、アクセス可能と判定され、アクセス可否情報をアクセス不可に変更された後に、指示されたデータ記憶領域にアクセスし、(4)第二の排他制御部は、第二のデータアクセス部により、指示されたデータ記憶領域に対してアクセスされた後に、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス可能に変更することを特徴とする。

【0010】また、第一のコンピュータシステムは、第

三のコンピュータシステムを有する第一のネットワークシステムに接続し、第一のサービス部は、第一のネットワークシステムを介して第三のコンピュータシステムに対してサービスを提供し、第二のコンピュータシステムは、第四のコンピュータシステムを有する第二のネットワークシステムに接続し、第二のサービス部は、第二のネットワークシステムを介して第四のコンピュータシステムに対してサービスを提供することを特徴とする。

【0011】また、第二のサービス部は、第一のサービス部が第一のネットワークシステムを介して第三のコンピュータシステムに対して提供するサービスと等価のサービスを、第二のネットワークシステムを介して第四のコンピュータシステムに対して提供することを特徴とする。

【0012】また、第一の排他制御部は、バスロック機能付きバスによって、アクセス可否情報記憶部に接続し、第一の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更する間、バスをロックし、第一の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス可能に変更する間、バスをロックし、第二の排他制御部は、上記バスロック機能付きバスによって、アクセス可否情報記憶部に接続し、第二の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更する間、バスをロックし、第二の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス可能に変更する間、バスをロックすることを特徴とする。

【0013】また、第一の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更する一連の動作を、一の命令で実行し、第二の排他制御部は、指示されたデータ記憶領域に対応するアクセス可否情報を取得し、指示されたデータ記憶領域に対してのアクセスの可否を判定し、アクセス可能と判定した場合には、指示されたデータ記憶領域に対応するアクセス可否情報をアクセス不可に変更する一連の動作を、一の命令で実行すること特徴とする。

【0014】また、第一のコンピュータシステムは、以下の要素を備えることを特徴とする。

(1) データの暗号化及び復号化に用いる暗号鍵を記憶する暗号鍵記憶部、(2) 暗号鍵を指定して暗号化を指

示された場合には、指定された暗号鍵を用いてデータを暗号化し、暗号鍵を指定して復号化を指示された場合には、指定された暗号鍵を用いてデータを復号化するデータ暗号化／復号化実行部、(3) 暗号鍵記憶部が記憶する暗号鍵を変更する暗号鍵再設定部、(4) 第一のデータアクセス部に、データ記憶領域からの暗号データの読み出しを指示し、データ暗号化／復号化実行部に、変更前の暗号鍵を指定して、読み出した暗号データの復号化を指示し、データ暗号化／復号化実行部に、変更後の暗号鍵を指定して、復号化したデータの再暗号化を指示し、第一のデータアクセス部に、再暗号化したデータを、元のデータ記憶領域へ書き込むことを指示するデータ再暗号化部。

【0015】この発明に係るクライアントは、ネットワークシステムに接続するクライアントであって、以下の要素を有することを特徴とする。

(1) 上記ネットワークシステムに接続する第一のコンピュータシステムであって、第二のコンピュータシステムとデータを共有する第一のコンピュータシステムに対して、共有データを送信し、また、共有データを受信する共有データ送信／受信部、(2) データ送信／受信部が送信する共有データを暗号化するデータ暗号化部、

(3) データ送信／受信部が受信した共有データを復号化するデータ復号化部。

【0016】また、データ共有コンピュータシステムは、第三のコンピュータシステムを有し、第三のコンピュータシステムは、第一のコンピュータシステムが接続する第一のネットワークシステムに接続し、第一のサービス部は、第一のネットワークシステムを介して第三のコンピュータシステムに対してサービスを提供し、第三のコンピュータシステムは、第一のサービス部が提供するサービスによってアクセスした共有データをキャッシュする共有データキャッシュ部を有することを特徴とする。

【0017】また、第一のサービス部は、第一の構成情報を用いて動作し、共有データ記憶部は、第一のサービス部が用いる第一の構成情報を記憶し、第二のコンピュータシステムは、他の記憶部を有し、第二のコンピュータシステムは、共有データ記憶部に記憶されている第一の構成情報を読み出し、読み込んだ第一の構成情報を他の記憶部に書き込む構成情報複製部を有し、第二のサービス部は、他の記憶部に書き込んだ第一の構成情報を更新し、更新した第二の構成情報を用いて動作することを特徴とする。

【0018】また、第一のコンピュータシステムは、以下の要素を備えることを特徴とする。

(1) 第一のコンピュータシステムによるユーザ認証の認証方式を記憶する認証方式管理部と、(2) 認証に用いるデータを予め記憶する認証データベース管理部と、(3) 認証要求と認証を受ける為のデータとを受け付け、

10

20

30

40

50

認証を受ける為のデータと、認証データベース管理部に予め記憶された認証に用いるデータとを用いて、認証方式管理部に記憶された認証方式により、ユーザ認証を行なう認証機能部。

【0019】また、データ共有コンピュータシステムは、バスを備え、第一のコンピュータシステムと、第二のコンピュータシステムと、共有データ記憶部と、アクセス可否情報記憶部とが上記バスに接続された共有メモリ型並列計算機であることを特徴とする。

【0020】

【発明の実施の形態】以下本発明を図面に示す実施の形態に基づいて説明する。尚、図1から図11に、主として各実施の形態におけるシステムの構成を示し、図12から図49に各実施の形態の動作に伴うデータフロー、処理フローやコマンドの構成等を示す。

実施の形態1. 本発明によれば、クライアントサーバー型のサービスであって、アプリケーションプログラムとして実現されているものであれば、その既存のプログラムにほとんど変更を加えることなく、ネットワーク毎にそのサービスを複製して、それぞれネットワーク上で利用することが可能となる。例えば、IMAP4 (internet message access protocol 4) によるメールサービス、HTTP (hypertext transport protocol) サーバーサービスなどのサービスがこれに該当する。本実施の形態では、ファイルサーバーのサービスを複製し、利用する例を説明する。

【0021】図1に、サービス複製システムのシステム構成図を示す。ここで、101は、構内LAN (local area network)、102は、インターネット、103は、LAN側サーバー、104は、共有ディスク、105は、インターネット側サーバー、106は、バスロック機能付きバス、107は、LAN上のクライアントである。

【0022】LAN側サーバー103とインターネット側サーバー105とは、それぞれに独立したサーバー装置であるが、構内に隣接して設置され、各々SCSI (small computer system interface) にて共有ディスク104に接続し、共有するように構成されている。尚、SCSI以外に、ファイバチャネル等のより長い接続経路を許す技術を使用して共有ディスク104と接続する場合には、必ずしもサーバー装置同士を隣接する必要はない。

【0023】バスロック機能付きバス106は、LAN側サーバー103とインターネット側サーバー105とに接続し、サーバー装置間の共有メモリ機構に使用されるように構成されている。

【0024】図2に、LAN側サーバー103とインターネット側サーバー105の各サーバー装置上に配置されるソフトウェアの構成図を示す。201は、アプリケ

ーションプログラム部、202は、ファイルシステム部、203は、ファイルサービス部、204は、ユーザー認証/認可管理部、205は、データ暗号/復号化実行部、206は、データ管理部である。

【0025】アプリケーションプログラム部201は、ユーザー認証/認可管理部204とファイルサービス部203を呼び出して、アプリケーションを実行するように構成されている。ファイルサービス部203は、ファイルシステム部202を呼び出すように構成されている。ファイルシステム部202は、データ管理部206を呼び出すように構成され、データ管理部206は、データ暗号/復号化実行部205を呼び出すように構成されている。尚、ファイルサービス部203のサービスは、オペレーティングシステムのカーネルコードとして実行され、その処理コンテキストは1アプリケーションとして与えられるように構成されている。

【0026】図3に、204ユーザー認証/認可管理部が、データ管理部206を用いて管理するユーザー認証/認可データベースのレコード例の図を示す。301は、ユーザーID、302は、そのユーザーのグループID、303は、そのユーザーのユーザーID、304は、そのユーザーの認証データ、305は、そのユーザーの共通秘密鍵である。ユーザーの共通秘密鍵は、データ管理部206がデータの暗号/復号化を行なう際に利用するものである。尚、ユーザー認証/認可管理部204は、ハッシュ関数によるパスワード参照の基本方式に加えて、チャレンジ方式と、ワンタイムパスワード方式を用意しており、ユーザー属性として認証方式の選択が可能のように構成されている。

【0027】図4に、データ管理部206の構成図を示す。401は、排他制御部、402は、データ暗号/復号化指示部、403は、データアクセス部である。排他制御部401は、バスロック機能付きバス106を用いて共有メモリ機構にアクセスし、共有ディスク104のセクタ単位で、排他制御を行なうように構成されている。データ暗号/復号化指示部402は、共有ディスク104に書き込むデータの暗号化と、共有ディスク104から読み出したデータの復号化を、データ暗号/復号化実行部205に指示するように構成されている。データアクセス部403は、共有ディスク104のセクタ単位で、読み出しと、書き込みをするように構成されている。

【0028】図5に、ロック中の共有ディスクセクタと共有メモリの状態の例の図を示す。501は、共有メモリ上のロックフィールド、502は、共有ディスク104上のセクタを示す。

【0029】次に、この構成における基本的な動作について説明する。まず、図12と図13を用いて、システムログインの処理について説明する。図12は、システムログインの処理フロー図である。図13は、システム

ログイン処理のデータフロー図である。

【0030】システムログインでは、ユーザー認証の処理を行ない（S1201）、ユーザー認証が成功した場合に、ログインセッションを生成する（S1202）。

【0031】次に、図14と図15を用いて、ファイルオープン処理について説明する。図14は、ファイルサービス部203によるファイルオープン処理の処理フロー図である。図15は、ファイルオープン処理のデータフロー図である。

【0032】ファイルサービス部203は、クライアント107のクライアントプログラム部からファイルオープン処理の処理要求を受けると（S1401、1501）、ユーザー認証を行ない（S1402、1502、1503）、ユーザー認証が成功した場合に、ファイルシステム部202にオープン処理を依頼する（S1403、1504）。オープン処理の結果、ファイルシステム部202からファイル管理データ（通常、vnodeと呼ばれる。）とクライアント認証キーを取得する（S1404、S1405、1505）。

【0033】ファイルサービス部203は、取得したクライアント認証キーを記憶し（S1406）する。尚、これ以降にクライアント107からファイルサービス部203へデータアクセスの要求がされた場合には、ファイルサービス部203は、クライアントからの処理要求メッセージに含まれるクライアント認証キーと、記憶しているクライアント認証キーを比較することによって認証処理を行なう（S1603、S2303）。つまり、ユーザー認証／認可管理部204によらず、ファイルサービス部203自身が認証を行なう。

【0034】ファイル管理データ（vnode）は、ファイルシステム部202によってファイル毎に管理されるデータであって、ファイルのアクセス権、サイズ、オープンカウント、シークポインタ、ファイルデータの配置されるディスクブロックアドレスなどの情報の管理に用いられる。尚、このファイル管理データ（vnode）は、ファイルサービス部203経由でアクセスする場合だけでなく、他のアプリケーションプログラムからファイルシステム部202に対してアクセスする場合にも用いられる。その場合、具体的にはファイルシステム部202に対して、ファイル管理データ（vnode）に基づいたリード、ライト、シーク等のシステムコールを行なう。ファイルシステム部202は、そのシステムコールを解釈し、該当するディスク領域へアクセスする。

【0035】ファイルサービス部203は、インデックスとクライアント認証キーとファイルオープン終了結果をクライアントプログラム部へ送信して（S1406、S1407、S1408、1506）、ファイルオープン処理を終了する。

【0036】次に、図16から図21を用いて、リード

の処理について説明する。図16は、ファイルサービス部203によるリードの処理フロー図である。図17は、リード要求メッセージの例を示す図である。図18は、ファイルシステム部202によるリードの処理フロー図である。図19は、データ管理部206によるリードの処理フロー図である。図20は、共有ディスク領域のリードセクタに対するロック取得の処理フロー図である。図21は、共有ディスク領域のリードセクタに対するロック開放の処理フロー図である。図22は、リード処理のデータフロー図である。

【0037】ファイルサービス部203は、UDP（user datagram protocol）の既知ポートをクライアントプログラム部に提供し、同ポートに対してクライアント103からの処理要求を受け付けることにより、ファイルサービスを行なう。クライアントプログラム部は、リードに相当する要求メッセージをファイルサービス部203に送信し、ファイルサービス部203は、メッセージを解釈してサービスを提供する（S1601、2201）。

【0038】リード要求メッセージは、図17のようなフォーマットで構成される。1701は、ファイル管理データ（vnode）へのポインタの配列へのインデックス、1702は、ユーザーID、1703は、クライアント認証キー、1704は、サービス内容（ここで、1はリードを意味する。）、1705は、リード開始セクタオフセット、1706は、リードセクタサイズである。

【0039】図16に示すように、ファイルサービス部203は、リード要求メッセージ中のクライアント認証キー1703を取得し（S1602）、ファイルオープン処理中に記憶した（S1406）クライアント認証キーと比較して、一致する場合には処理を続行する（S1603）。

【0040】リードするデータ領域が、共有ディスク104上の共有ディスクデータ領域の場合には、サーバー装置内の他のファイルシステムではなく、その共有データ領域を管理するデータ管理部206を用いるファイルシステム部202を選択する（S1605、S1607）。

【0041】ファイルサービス部203は、メモリ領域を確保し（S1608）、ファイルシステム部202にリード要求を出す（S1609、2202）。このとき、同時にファイル管理データ（vnode）へのポインタ、リード開始セクタオフセット、リードセクタサイズ、確保したメモリ領域の先頭アドレスを渡す。通常、ユーザーからのファイルシステム部202へのアクセスは、システムコール経由で行なわれるが、この場合のリード要求では、ファイルシステム部202の内部関数を利用して行われる。

【0042】図18に示すように、ファイルシステム部

10

20

30

40

50

202は、リード要求を受けると（S1801、2202）、ファイル管理データ（vnode）中のリード開始セクタオフセットを、データ管理部206で管理するリードセクタアドレスに変換し（S1802）、データ管理部206に対してリード要求を出す（S1803、2203）。このとき同時に、ユーザーID、リードセクタアドレス、リードセクタサイズ、メモリ領域の先頭アドレスを渡す。

【0043】図19に示すように、データ管理部206は、リード要求を受付け（S1901、2203）、排他制御部401により、共有ディスク領域のリードセクタのロック取得を行なう（S1902）。

【0044】排他制御部401がアクセスする共有メモリ機構は、バスロック機能付きバス106を用いて、バスロックと1ビット毎のデータ参照更新とをできるだけハードウェア構成で実現されている。排他制御部401は、このハードウェア構成を利用し、共有メモリ機構上のバイトアドレスを共有ディスク上のセクタアドレスにマッピングしている。

【0045】図20の示すように、排他制御部401は、リードセクタアドレスとリードセクタサイズを受けると（2204）、バスロックを施して（S2001、2205）、連続するリードセクタに対応するすべての共有メモリ機構上のバイトアドレス、つまりロックフィールドをチェックする（S2002、2206）。リードセクタのうち一つでも使用中であることを示すロックフィールドがあれば、バスロックを解放して（S2003、2205）、一定時間の休眠し（S2004）、その後リトライを繰り返す。総てのロックフィールドがリードセクタの未使用を示している場合には、排他制御部401は、バスロック状態のまま、それらのロックフィールドに1（1は、ロックフィールドに対応するセクタが使用中であることを示す。）を書き込む（S2005、2206）。その後、バスロックを解放する（S2006、2205）。

【0046】図5に、ロック中の共有ディスクセクタと共有メモリの状態の例を示す。共有メモリのロックフィールド501の先頭は、共有ディスク上の1番目のセクタと対応していることを意味する。この例では、7番目から11番目のロックフィールドが使用中となっている。そのため、7番目から11番目のロックフィールドに対応する共有ディスク上の7セクタから11セクタまでは、ロック状態にあり、ロック取得したユーザー以外は、これらのセクタに対してアクセスすることができないことを意味している。

【0047】データ管理部206は、データアクセス部403により、リードセクタからディスクデータの読み出し（S1903、2208、2209）、アドレスを指定されたメモリ領域に格納する（2210）。

【0048】データ管理部206は、読みだしが終了す

ると、排他制御部401により、ロックの解放を行なう（S1904）。ロックの解放は、図21に示すように、バスロックを取得した上で（S2101、2205）、ロックフィールドに0を書き込むことにより行なわれる（S2102、2206）。その後、バスロックは解放される（S2103、2205）。

【0049】データ管理部206は、データ暗号/復号化指示部402により、メモリ領域に読み込んだデータを復号化する（S1905）。データ暗号/復号化指示部402は、ファイルシステム部202から与えられたユーザーIDを指定して、ユーザー認証/認可管理部204からそのユーザーの共通秘密鍵305を得る。データ暗号/復号化指示部402は、この共通秘密鍵305を用いて、データ暗号/復号化実行部に復号化を実行させる（2212、2213、2214）。復号化したデータをメモリ領域に書き込み（S1906、2215）、ファイルシステム部202へリターンする（S1907、2216）。

【0050】ファイルシステム部202は、ファイルサービス部203へリターンする（S1805、2218）。

【0051】ファイルサービス部202は、リード要求を受けたクライアントプログラムのポートに読み出したデータを返送して、リード処理を終了する（S1611、2219）。

【0052】次に、図23から図29を用いて、ライトの処理について説明する。図23は、ファイルサービス部203によるライトの処理フロー図である。図24は、ライト要求メッセージの例を示す図である。図25は、ファイルシステム部202によるライトの処理フロー図である。図26は、データ管理部206によるライトの処理フロー図である。図27は、共有ディスク領域のライトセクタに対するロック取得の処理フロー図である。図28は、共有ディスク領域のライトセクタに対するロック開放の処理フロー図である。図29は、リード処理のデータフロー図である。

【0053】ファイルサービス部203は、リードの処理と同様に、ライト要求メッセージを受け付ける（S2301、2901）。ライト要求メッセージは、図24のようなフォーマットで構成される。2401は、ファイル管理データ（vnode）へのポインタの配列へのインデクス、2402は、ユーザーID、2403は、クライアント認証キー、2404は、サービス内容（ここで、0はライトを意味する。）、2405は、ライト開始セクタオフセット、2406は、ライトセクタサイズ、2407は、ライトデータ列である。

【0054】ライト要求は、リードの処理と同様に、ファイルシステム部202に渡され（S2309、2902）、ファイルシステム部202は、データ管理部206に、ユーザーID、ライトセクタアドレス、ライトセ

25

クタサイズ、ライトデータを格納したメモリ領域の先頭アドレスを渡す(S2503、2904)。リードの処理と同様に、データ暗号/復号化指示部205は、ユーザーIDに基づいてユーザーの共通暗号鍵305を得て、データ暗号/復号化実行部205に、データの暗号化を実行させる(S2603、2909~2912)。また、リードの処理と同様に、排他制御部401は、共有ディスク領域のライドセクタのロック取得を行ない(S2604、2906、2907)、データアクセス部403は、暗号データを書き込み(S2605、2915、2916)、その後排他制御部401は、ロックを解放する(S2606、2906、2907)。

【0055】本実施の形態によれば、例えば企業内ネットワークとインターネットで安全にデータを共有でき、ネットワーク毎にサービスを複製して利用することができる。

【0056】実施の形態2. 次に、共有メモリ型並列計算機上でネットワーク毎にパーティショニングされたシステムについて説明する。図6は、並列計算機のシステム構成例である。ここで、601、602は、CPU、603、604は、イーサネットコントローラ、605は、メモリ、606は、ディスクコントローラ、607は、ディスクであり、608は、メモリバスである。

【0057】メモリバス608には、CPU601、602、イーサネットコントローラ603、604、メモリ605、ディスク607が接続されている。CPUはテストアンドセット命令を備え、CPUから各デバイスへのアクセス、デバイスからCPUへの割り込みは、メモリバス上の特定のアドレスにマッピングされたレジスタ経由で行なわれる様に構成されている。テストアンドセット命令については、後述する。

【0058】メモリ605とディスク607の一部には、共有メモリ領域と共有ディスク領域が設けられている。LANに接続されるイーサネットコントローラ603に接続され、LANに所属するCPU601と、インターネットに接続されるイーサネットコントローラ604に接続され、インターネットに所属するCPU602とは、仮想空間で隔離され、各ネットワークに固有のメモリ領域、および、お互いのイーサネットコントローラにアクセスすることはできないように構成されている。

【0059】次に、図30を用いて、この構成における基本的な動作について説明する。このシステムは、リセットされると、CPU601のみが、仮想記憶をディスエーブルした状態でROMコードの実行を始める。この時、CPU602はディスエーブル状態となっている。

【0060】CPU601は、メモリプロブチェックを実行して使用可能なメモリ量を得て(S3001)、ブートコードをロードし、実行する(S3002)。ブートコードの実行により、メモリ量をチェックして、図7に示すようにメモリ領域を分割する(S3003)。

図7は、メモリ区分の例である。707は、LANに所属するCPU601の使用するメモリ領域、708は、インターネットに所属するCPU602の使用するメモリ領域、709は、排他制御のために使用する共有メモリ領域である。

【0061】メモリ領域の分割を決定すると、次に各々のCPUの仮想空間を形成するページテーブルのセットアップを行なう(S3004)。CPU601のメモリ領域707では、イーサネットコントローラ603のレジスタ領域へのページテーブルエントリ701、共有ディスクのコントローラレジスタ領域へのページテーブルエントリ702、共有メモリ領域へのページテーブルエントリ703、および、CPU601のカーネルコード使用領域のページテーブルエントリをセットアップする。同様に、CPU602のメモリ領域708では、イーサネットコントローラ604のレジスタ領域へのページテーブルエントリ704、共有ディスクのコントローラレジスタ領域へのページテーブルエントリ705、共有メモリ領域へのページテーブルエントリ706、および、CPU602のカーネルコード使用領域のページテーブルエントリをセットアップする。

【0062】カーネルの仮想空間は、図7に示したページテーブルエントリを除き、2つの領域で同等にセットアップされ、同一のカーネルコードが同一のカーネル仮想アドレスにロードされる。CPU602は、仮想記憶をイネーブルし、カーネルコードのスタートアドレスから実行を開始する。また、CPU601も、仮想記憶をイネーブルし、自身のスタートアドレスにジャンプして、カーネルコードの実行を開始する(S3006、S3007)。

【0063】実施の形態1で示したソフトウェアと同一のソフトウェアが、各々のCPUで実行されるが、排他制御部401の処理方式については、実施の形態1と異なり、本実施の形態の特徴を有する。実施の形態1では、共有メモリバスのバスロック機構を用いて、共有ディスク領域のライドセクタのロック取得とロック解放の処理を行なったが、本実施の形態では、図31に示すように、共有メモリ605上のロックフィールドに対してのロック取得とロック解放の処理をテストアンドセット命令によるロック機構を用いて行なう。テストアンドセット命令とは、メモリ上のデータに対してアトミックに参照更新を行なえる命令である。図32に示すように、ロック取得の処理の場合は、当該ロックフィールドに対して1をセットすることにより行なう(S3201)。そして、同命令で得られた値が0である場合には、ロック取得処理の成功を意味し(S3203)、1の場合には、すでに他者がロック取得済みであったため、ロック取得処理が失敗したことを意味する(S3204)。また、ロック解放の処理は、テストアンドセット命令でロックフィールドを0に書き戻すことで行なわれる。

【0064】このように本実施の形態によれば、共有メモリ型並列計算機上でネットワーク毎にパーティショニングされたシステムを実現し、各々のネットワークから他者ネットワークへの侵害を排除することによって、システムの安全性を向上させることができる。

【0065】実施の形態3. 本実施の形態では、複数のネットワークから参照できる共有ディスク上の暗号化データを、定期的に異なるキーを用いて再暗号化する機構について説明する。

【0066】実施の形態1で説明したように、ユーザー認証/認可管理部203は、図3に示すような共通秘密暗号鍵305を含むレコードからなるユーザー認証/認可データベースを管理し、ユーザーが登録時に暗号鍵を設定することにより、データを暗号化して保存することを可能にしている。本実施の形態では、それに加えてユーザーがシステムの提供する暗号鍵再設定/再暗号化コマンド(setenckeyコマンドという。)を利用することにより、暗号鍵の変更、およびその暗号鍵によるデータの再暗号化を行なうことを可能にする。

【0067】setenckeyコマンドは、安全性を高めるために、イントラネット側のサーバー105、あるいはオペレーティングシステムにのみ用意される。また、さらに安全性を高めるためには、後述する再暗号化API(application programming interface)をイントラネット側サーバー105にのみ備える構成とすることも有効である。

【0068】次に、図33から図38を用いて、暗号鍵再設定及びデータの再暗号化を実行する基本的な動作について説明する。ユーザーは、ユーザー認証を経て、イントラネット側サーバー105にログインを実行し(S3301)、図34のようなsetenckeyコマンドを実行させる(S3302)。ここで、3401は、新暗号鍵を意味する。

【0069】図35を用いてsetenckeyの処理を説明する。setenckeyコマンドの実行により、ユーザー認証/認可管理部204は、ユーザー認証/認可データベース中のレコードの暗号鍵を指定された新暗号鍵に変更する(S3501、S3502)。

【0070】その後、ファイルシステムに対して、図36に示すような特殊APIシステムコールsetuseratrを発行する(S3503)。3601は、ユーザーID、3602は、旧暗号鍵、3603は、新暗号鍵であり、図3に示すレコードを例とすると、ユーザーsakakuraの旧暗号鍵01280909を新暗号鍵01010101に変更せよという意味である。

【0071】図37を用いて、setuseratrの処理を説明する。システムコールsetuseratrの実行により、ファイルシステム部202は自らが管理するファイルのうちそのユーザーがオーナーであるファイルを全検索する(S3701)。データ管理部206

に対して、発見したそのユーザーのファイルが使用するセクタを対象に、再暗号化コマンドreencを発行する(S3702)。具体的には、再暗号化コマンドreencに、旧暗号鍵、新暗号鍵、更新セクタチャンク数、セクタアドレス、とセクタサイズのセクタチャンク数分のエントリを有する配列を引数として渡してコールする。

【0072】図38を用いて、reencの処理について説明する。reencの処理では、実施の形態1で述べたデータ管理部206によるリードやライトのオペレーションと同様に、配列で示された当該セクタすべてのロックを取得する(S3801)。その後すべてのセクタデータに対し読み出しを行ない(S3802)、データ暗号/復号化機能を使用して旧暗号鍵で復号した後(S3803)、新暗号鍵で再暗号化して(S3804)、当該ディスクへの書き戻しを行なう(S3805)。すべての当該セクタにつき書換えが終了すると、取得したすべてのロックを解放し(S3806)、ファイルシステム部202にリターンする。

【0073】システムコールを終了し、ユーザー認証/認可管理部204にリターンし、setenckeyコマンドの実行を終了する。

【0074】前述の実施の形態におけるサーバー装置は、ユーザー認証により第三者からの不法なアクセスからシステムを保護するように構成されているが、本実施の形態にかかる再暗号化機構は、万が一第三者に不法なログインを許してしまった場合に備え、データ秘匿性を高めることができる点で有効である。

【0075】実施の形態4. 本実施の形態では、サーバー上に保管されている暗号化データをクライアント上で復号化し、データの秘匿安全性を向上させる形態について説明する。

【0076】図8に、サーバー装置を利用するクライアントのソフトウェア構成図を示す。801は、クライアントプログラム上で動作するクライアント側アプリケーションプログラム部、802は、実施の形態1、2のファイルサービス部203に対するクライアントとしての機能を含むクライアント側ファイルシステム部、803は、データ暗号/復号化実行部205と同等の機能を有するクライアント側データ暗号/復号化実行部である。例えば、クライアントに携帯端末を用いる場合には、一つのクライアントに対してユーザーは一人しかいないことになる。

【0077】クライアント側アプリケーションプログラム部801は、実施の形態1のサーバー上のアプリケーションプログラム部と同様にクライアント側ファイルシステム部802に対してファイルの読み書き操作を行なうように構成されている。

【0078】次に、図39から図41を用いて本実施の形態における基本的な動作について説明する。図39

は、オープン処理のデータフロー図である。クライアント側ファイルシステム部802は、openシステムコール3901を解釈し、サーバー装置上のファイルサービス部203のUDP (user datagram protocol) の既知ポートに対して、「暗号/復号化なし」の属性でオープンメッセージを送信する(3902)。vnode中に「暗号/復号化不要」のデータが含まれる以外は、実施の形態1と同様に処理される。「暗号/復号化不要」の属性でオープンしている間には、「暗号/復号化必要」な処理は許されず、逆に「暗号/復号化必要」の属性でオープンしている間には、「暗号/復号化不要」な処理は許さない。

【0079】図40は、リード処理のデータフロー図である。クライアント側ファイルシステム部802は、ファイルオープンに引続きリードシステムコールを受けると(4001)、ファイルサービス部203にリード要求メッセージを送信する(4002)。ファイルサービス部203は、ファイルシステム部202にリード要求を出す(4003)。ファイルシステム部202は、vnodeが「暗号/復号化不要」となっているので、データ管理部206に対して、復号化無しリード要求を発行する(4004)。データ管理部206からの復号化無しリード要求に対する処理は、復号化処理を行なわない点を除き実施の形態1で説明したリード処理と全く同じに動作する。このようにして、暗号化されたままのデータが、クライアント107に、実施の形態1での返送メッセージと同じ態様で返送される(4016)。

【0080】クライアント側では返送された暗号化データを受けると、クライアント側ファイルシステム部802が、コンフィグレートされた暗号鍵を用いてデータ暗号/復号化実行部803に復号化を実行させる(4016)。クライアント側ファイルシステム部802は、復号化されたデータをクライアント側アプリケーションプログラム部801に返してリード処理を終了する(4018)。

【0081】図41は、ライト処理のデータフロー図である。クライアント側ファイルシステム部802は、ライトシステムコールを受けると(4101)、暗号鍵を用いて受けとったデータをデータ暗号/復号化実行部803に暗号化させる(4102、4103)。クライアント側ファイルシステム部802は、暗号化されたデータとライト要求メッセージをファイルサービス部203に送信する(4104)。ファイルサービス部203は、ファイルシステム部202へライト要求を発行する(4106)。ファイルシステム部202は、データ管理部206に対して暗号化無しライト要求をコールする(4107)。実施の形態1で説明したデータ管理部206は、暗号化せず、そのままデータを書き込む(4113、4114)。ファイルサービス部203は、処理の完了をクライアント107に報告する(4117)。

【0082】このようにクライアント上にデータの暗号/復号化機能を置くことにより、データの秘匿安全性を向上することができる。特に、携帯クライアント端末から無線通信にてサーバと通信する場合に、データの秘匿安全性を確保することができる点で有効である。

【0083】実施の形態5。本実施の形態では、遠隔地からインターネットを介して、本発明に係る複製サービスを利用する場合に、データ転送遅延を小さくするシステムについて説明する。具体的には、代理サーバーを設け、実施の形態1で説明したファイルサービスのデータキャッシュ機能を実現する例を説明する。

【0084】図9は、実施の形態5に係るシステム構成を示す図である。105は、実施の形態1で説明したインターネット側サーバー(複製サーバー)105、901は、代理サーバー、902は、LAN、903と904は、クライアントである。クライアント903、904は、インターネット102を介してインターネット側サーバー105からサービスの提供を受ける。

【0085】代理サーバー901が提供するファイルサービスは、クライアント903、904からみて、インターネット側サーバー105のファイルサービス部203に直接接続した場合のファイルサービスと全く同等になるように構成される。そのため代理サーバー901は、インターネット側サーバー105のファイルサービス部203が提供しているUDPの既知ポートと同一番号のポートをクライアント903、904に対して提供している。

【0086】次に、この構成における基本的な動作について説明する。まず、オープン処理について説明する。

図42は、オープン処理のデータフロー図である。4251は、クライアントプログラム部、4252は、代理サーバー側ファイルサービス部である。

【0087】クライアントプログラム部4251は、代理サーバー901の前記既知ポートにファイルオープンメッセージを送信する(4201)。代理サーバー側ファイルサービス部4252は、ファイルオープンメッセージを受けると、内部データ(ファイルエントリ、セクタ管理テーブル及びセクタデータ領域)を用意する。

【0088】図10は、内部データ(ファイルエントリ、セクタ管理テーブル及びセクタデータ領域)の構成を示す図である。1001は、ファイルエントリである。そのうち、1002は、ユーザーIDフィールド、1003は、ファイル名フィールド、1004は、クライアント認証キーフィールド、1005は、ファイルオープン属性フィールド、1006は、ファイルのオープンアカウントフィールド、1007は、先頭セクタの管理テーブルへのポインタフィールドである。また、セクタ管理テーブルは、1008のファイルのセクタ番号、1009の次管理テーブルへのポインタ、1010のセクタデータ領域へのポインタから構成される。1011

は、セクタデータ領域である。

【0089】代理サーバー側ファイルサービス部4252は、ファイルオープンメッセージ中のユーザーのIDとオープンするファイル名を、それぞれユーザーIDフィールド1002とファイル名フィールド1003に格納する(4202)。また、ファイルオープン属性をファイルオープン属性フィールド1005に格納する(4202)。このファイルオープン属性には、実施の形態4で説明した「暗号/復号化必要」あるいは「暗号/復号化不要」の属性が含まれる。

【0090】ファイルオープンメッセージは、そのままインターネット側サーバー105のファイルサービス部203に転送され(4203)、代理サーバー側ファイルサービス部4252は、ファイルサービス部203からの返送メッセージ中にあるクライアント認証キーをクライアント認証キーフィールド1004に格納する(4202)。また、本ファイルのオープンカウントは、ファイルのオープンアカウントフィールド1006に格納される(4202)。

【0091】次に、リード処理について説明する。図43は、リード処理の処理フロー図である。図44は、リード処理のデータフロー図である。代理サーバー側サービス部4252は、クライアントプログラム部4251からのリード要求メッセージを受けとると(S4301、4401)、先頭セクタの管理テーブルへのポインタフィールド1007をチェックする(S4302、4402)。このフィールドに0xffffffffが格納されている場合(先頭セクタの管理テーブルへのポインタがセットされていないことを意味する。)には、このファイルは、リード処理が実行されていないと判断し、クライアントプログラム部4251からのメッセージをインターネット側サーバー105のファイルサービス部203に転送する(S4303、4403)。

【0092】代理サーバー側サービス部4252は、リードデータを取得し(S4304、4404)、返送メッセージをクライアントプログラム部4251に転送する(S4305、4405)。

【0093】代理サーバー側サービス部4252は、図10に示すように必要なセクタデータ領域1011とそれに対応するセクタ管理テーブル1008、1009、1010を確保する(S4306、S4307、4406、4407)。先頭セクタの管理テーブルへのポインタフィールド1007に、先頭セクタの管理テーブルへのポインタを格納し、(S4308、4408)。ファイルのセクタ番号フィールド1008に、対応するファイルのセクタ番号を格納し(S4309、4407)、セクタデータ領域へのポインタフィールド1010に、セクタデータ領域へのポインタを格納し(S4310、4407)、セクタデータ領域1011に返送メッセージから得たリードデータを格納する(S4311、44

06)。

【0094】2以上のセクタデータ領域を必要とする場合には(S4312)、次管理テーブルへのポインタフィールド1009に、次管理テーブルへのポインタを格納し(S4313、4407)、これによって管理テーブルをリンクし、管理テーブルが最終の場合には(S4312)、次管理テーブルへのポインタフィールド1009に、0xffffffffを格納する(S4314、4407)。

10 【0095】これ以降代理サーバーへのこのファイルに対するリード要求が発生した場合に、図10に示すキャッシュ上に既に該当するセクタが存在すれば(S4302)、そのデータをそのまま利用する(S4315～S4319)。セクタが存在しないければ(S4320)、不足分のセクタデータをインターネット側サーバー105のファイルサービス部203に要求して(S4303)、既存セクタデータのリンクに挿入する(S4313、S4309～S4312)。リード要求にあるセクタがすべて揃った時点で、ファイルサービス部203が生成するのと同じ形態のリード要求返送メッセージを作成し、クライアントプログラム部に返す(4205、4405)。

【0096】次にライト処理について説明する。図45は、ライト処理の処理フロー図である。図46は、ライト処理のデータフロー図である。クライアントプログラム部4251からのライト要求メッセージを代理サーバー側ファイルサービス部4252が受けとると(S4501、4601)、代理サーバー側ファイルサービス部4252は、このメッセージをインターネット側サーバー105のファイルサービス部203に転送する(S4502、4602)。すでにこのファイルのファイルエントリ1001に、ライトするセクタのデータが保存されていれば(S4504、4604)、それらのセクタに対してクライアントプログラム部4251からのライト要求メッセージ中のセクタデータで上書きし(S4505、4605)、当該セクタのセクタデータ領域が確保されていないければ、新たなセクタデータ領域を確保して(S4507、4606、4607)、これらのリンクに挿入する(S4508、4607、4608)。

40 【0097】次にファイルの無効化の処理について説明する。図47は、ファイル無効化処理のデータフロー図である。あるファイルが代理サーバー901によってキャッシュされている場合に、LAN側サーバー103から共有ディスク104上の対応するファイルの内容が更新されると、代理サーバー901上のファイルデータと共有ディスク104上の対応するファイルデータは、同一でなくなる。このような場合のファイルデータの一貫性維持のコントロールに関しては、クライアント903、904に任される。そのため、クライアント側アップ
50 リケーション部801は、代理サーバー901上のキャ

ッシュされたファイルデータを無効化したい場合に、クライアント側ファイルシステム部802に対して、無効化したいファイルを指定してfcntlシステムコールの無効化コマンドを発行する(4701)。

【0098】クライアント側ファイルシステム部802は、無効化コマンドを解釈し、代理サーバー901に対し無効化要求を出す(4702)。図48は、無効化要求メッセージの例を示す図である。

【0099】代理サーバー側ファイルサービス部4252は、無効化要求メッセージを受けると、自らが管理するファイルエントリを検索し(4703)、無効化するファイルのファイルエントリのファイルオープン属性1005を0xfffffにて初期化しキャッシュデータを無効化する(4704)。これにより、再びこのファイルに対するリード要求があった場合に、改めてインターネット側サーバー105のファイルサービス203からファイルデータを取得するようになる。

【0100】ここで問題視するデータ転送遅延は、インターネット接続の距離が大きくなるにつれて増大する。例えば、日本とアメリカ西海岸では到達に0.2秒ほどかかる。この遅延時間を吸収するため、本発明は有効である。

【0101】実施の形態6。上述のように本発明を適用することにより、複数のネットワークに対して共通のファイルサービスが提供できる。このようなファイルサービスが提供するネットワーク間の共有ファイルを利用して、ファイル上のデータを基に動作するサーバーサービスを、従来のサーバープログラムを変更することなく提供することができる。例えば、IMAP4(inter net message access protocol 4)メールサービスを複製すると、このサーバー機能がSMTPにてイントラネット内でメールデータを受けとり、共有ディスク上にサーバーの管理するデータとしてメールデータを保管する。このデータは共有ディスクに管理されるので、このメールデータを基にイントラネット、インターネット上でIMAP4サービスを提供できる。これにより、IMAP4メールサービスのユーザーは、イントラネット(例えば、社内)からでも、インターネット(例えば、出先)からでもイントラネットのユーザーのメールアカウントに届いたメールを読ん

で処理することができるようになる。

【0102】ところが、同じサーバープログラムを使用するものの、IMAP4サーバーの設定に関して、イントラネット側ではメール取り込みが必要なものに対して、インターネット側ではメール取り込みが不要となる。つまり、設定ファイルの一部について、各ネットワーク毎に独自に設定する必要が生じ、別個に設定ファイルを設定しなければならない場合がある。

【0103】そのために本実施の形態では、そのような設定に必要なファイルローカライズ機構について説明す

る。サーバー装置の管理者は、ローカライズの必要なファイルに関して、以下のようなコマンドを出す。

Localize afile

具体的には、設定ファイルをオープンした後、設定ファイルを指定してfcntlシステムコールにて上記コマンドを発行する。

【0104】図49に、Localizeコマンド処理のフロー図を示す。ファイルシステム部202は、ファイルシステム部202が管理している非共有ディスク領域に、新たなセクタ領域を確保し(S4901)、データ管理部206から設定ファイルのセクタデータを読み出して(S4902)、確保したセクタ領域に読み出したセクタデータを書き込む(S4903)。このようにして、ファイルデータを非共有領域にコピーする。新たに確保したセクタを管理するinodeを参照するよう設定ファイルのvnodeを更新することにより(S4904)、ファイルシステム部は共有領域上のファイルのローカライズを行なう。

【0105】このようにして、ネットワーク毎にサービスの構成情報を独自に更新管理することが可能となる。

【0106】実施の形態7。本実施の形態では、本発明に係るサービス複製サーバー装置に関して、サーバー装置を構成するサブネットワーク毎にそのネットワークで必要とされる強度の認証機構を、必要に応じて構成することを可能とした認証機構について説明する。例えばイントラネットに関しては、一般に安全性確保のために外部のネットワークから厳重に保護されており、イントラネット内ではそれほど高い認証強度は要求されない。一方インターネットでは、常に外部の脅威に晒されており、高い認証強度が要求される。

【0107】図11に本実施の形態に係るユーザー認証/認可管理部の構成図を示す。1101は、認証機能部、1102は、認可方式管理部、1103は、認証/認可データベース更新管理部、1104は、認証/認可データベース管理部である。これらの構成により、各々のサブネットワークが必要とする認証強度の認証機能をサブネットワーク毎に構成することができる。

【0108】認証機能部1101は、ユーザーからの認証要求を受けて認証を行なう。このとき、認証機能部1101は、認証方式管理部1103が管理する認証方式に従い、認証/認可データベース管理部1104から認証データを得て、照合することによって認証を行なう。

【0109】システム管理者は、認証方式管理部1102にサブネットワークが必要とする認証強度にふさわしい認証機能を導入設定しておくことができる。例えば、イントラネットに関しては、UNIX等で広く普及しているMD5(messagedigest algorithm 5)のようにハッシュ関数認証を持った認証機能を導入設定し、一方インターネットに関しては、ワンタイムパスワードを用いた認証機能を導入設定するこ

とができる。

【0110】各認証機能は、認証機能部1101から認証検証すべきデータを得て、認証/認可データベース管理部1104から認証データを得て、認証するインターフェースを備えている。また、各認証機能は、共通の認証データを使用するよう構成されている。

【0111】認証/認可データベースは、各ネットワーク間で共有される。従って、システムのユーザー管理を行なうシステム管理者は、いずれかのサブネットワーク上の認証/認可データベース更新管理部1103に対して更新すれば足り、その更新内容は自動的にすべてのネットワークの認証機能に対して反映される。

【0112】

【発明の効果】本発明により、例えば企業内ネットワークとインターネットのように異なるネットワーク間で安全にデータを共有でき、ネットワーク毎にサービスを複製して利用することができる。

【0113】本発明では、共有メモリ型並列計算機上でネットワーク毎にパーティショニングされたシステムを実現しているので、各々のネットワークから他者ネットワークへの侵害を排除することによって、システムの安全性を向上させることができる。

【0114】本発明では、再暗号化機構により、万が一第三者に不法なログインを許してしまった場合に備え、データ秘匿性を高めることができる。

【0115】本発明では、クライアント上でデータを暗号/復号化することにより、データの秘匿安全性を向上することができる。特に、携帯クライアント端末から無線通信にてサーバと通信する場合に、データの秘匿安全性を確保することができる点で有効である。

【0116】本発明では、インターネット接続の距離が大きくなるにつれて増大するデータ転送遅延を吸収することができる。

【0117】本発明により、ネットワーク毎にサービスの構成情報を独自に更新管理することができる。

【0118】本発明により、サブネットワーク毎に必要なとされる強度の認証機構を用いることができる。

【図面の簡単な説明】

【図1】 実施の形態1に係るサービス複製システムのシステム構成図である。

【図2】 実施の形態1に係る各サーバ装置上に配置されるソフトウェアの構成図である。

【図3】 実施の形態1に係るユーザ認証/認可データベースのレコード例の図である。

【図4】 実施の形態1に係るデータ管理部の構成図である。

【図5】 実施の形態1に係るロック中の共有ディスクセクタと共有メモリの状態の例の図である。

【図6】 実施の形態2に係る並列計算機のシステム構成例を示す図である。

【図7】 実施の形態2に係るメモリ区分の例の図である。

【図8】 実施の形態4に係るクライアントソフトウェア構成図である。

【図9】 実施の形態5に係るシステム構成を示す図である。

【図10】 実施の形態5に係る内部データの構成を示す図である。

10 【図11】 実施の形態7に係るユーザ認証/認可管理部の構成図である。

【図12】 実施の形態1に係るシステムログインの処理フロー図である。

【図13】 実施の形態1に係るシステムログイン処理のデータフロー図である。

【図14】 実施の形態1に係るファイルオープン処理のフロー図である。

【図15】 実施の形態1に係るファイルオープン処理のデータフロー図である。

20 【図16】 実施の形態1に係るファイルサービス部によるリードの処理フロー図である。

【図17】 実施の形態1に係るリード要求メッセージの例を示す図である。

【図18】 実施の形態1に係るファイルシステム部によるリードの処理フロー図である。

【図19】 実施の形態1に係るデータ管理部によるリードの処理フロー図である。

【図20】 実施の形態1に係る共有ディスク領域のリードセクタに対するロック取得の処理フロー図である。

30 【図21】 実施の形態1に係る共有ディスク領域のリードセクタに対するロック開放の処理フロー図である。

【図22】 実施の形態1に係るリード処理のデータフロー図である。

【図23】 実施の形態1に係るファイルサービス部によるライトの処理フロー図である。

【図24】 実施の形態1に係るライト要求メッセージの例を示す図である。

【図25】 実施の形態1に係るファイルシステム部によるライトの処理フロー図である。

40 【図26】 実施の形態1に係るデータ管理部によるライトの処理フロー図である。

【図27】 実施の形態1に係る共有ディスク領域のライトセクタに対するロック取得の処理フロー図である。

【図28】 実施の形態1に係る共有ディスク領域のライトセクタに対するロック開放の処理フロー図である。

【図29】 実施の形態1に係るリード処理のデータフロー図である。

【図30】 実施の形態2に係る基本的な動作を示す図である。

50 【図31】 実施の形態2に係るテストアンドセット命令によるロック機構を示す図である。

【図32】 実施の形態2に係るロック取得結果を判断するフロー図である。

【図33】 実施の形態3に係るサーバ側の処理フロー図である。

【図34】 実施の形態3に係るsetenckeyコマンドのフォーマット図である。

【図35】 実施の形態3に係るsetenckeyの処理フロー図である。

【図36】 実施の形態3に係るsetuseratrのフォーマット図である。

【図37】 実施の形態3に係るsetuseratrの処理フロー図である。

【図38】 実施の形態3に係るreencの処理フロー図である。

【図39】 実施の形態4に係るオープン処理のデータフロー図である。

【図40】 実施の形態4に係るリード処理のデータフロー図である。

【図41】 実施の形態4に係るライト処理のデータフロー図である。

【図42】 実施の形態5に係るオープン処理のデータフロー図である。

【図43】 実施の形態5に係るリード処理の処理フロー図である。

【図44】 実施の形態5に係るリード処理のデータフロー図である。

【図45】 実施の形態5に係るライト処理の処理フロー図である。

【図46】 実施の形態5に係るライト処理のデータフロー図である。

【図47】 実施の形態5に係るファイル無効化処理のデータフロー図である。

【図48】 実施の形態5に係る無効化要求メッセージの例を示す図である。

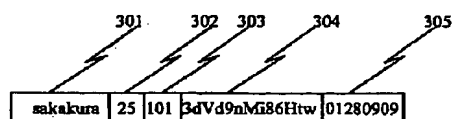
【図49】 実施の形態6に係るLocalizeコマンド処理のフロー図である。

【符号の説明】

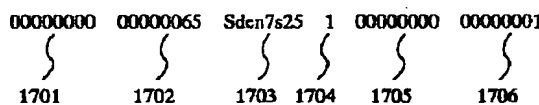
101 構内LAN (local area network)、102 インターネット、103 LAN側サーバー、104 共有ディスク、105 インターネ

ット側サーバー、106 パスロック機能付きバス、107 クライアント、201 アプリケーションプログラム部、202 ファイルシステム部、203 ファイルサービス部、204 ユーザー認証/認可管理部、205 データ暗号/復号化実行部、206 データ管理部、301 ユーザーID、302 ユーザーのグループID、303 ユーザーID、304 ユーザーの認証データ、305 共通秘密鍵、401 排他制御部、402 データ暗号/復号化指示部、403 データアクセス部、501 共有メモリ上のロックフィールド、502 共有ディスク上のセクタ、601、602 CPU、603、604 イーサネットコントローラ、605 メモリ、606 ディスクコントローラ、607 ディスク、608 メモリバス、701 イーサネットコントローラのレジスタ領域へのページテーブルエントリ、702 共有ディスクのコントローラレジスタ領域へのページテーブルエントリ、703 共有メモリ領域へのページテーブルエントリ、704 イーサネットコントローラのレジスタ領域へのページテーブルエントリ、705 共有ディスクのコントローラレジスタ領域へのページテーブルエントリ、706 共有メモリ領域へのページテーブルエントリ、707 LANに所属するCPUの使用するメモリ領域、708 インターネットに所属するCPUの使用するメモリ領域、709 排他制御のために使用する共有メモリ領域、801 クライアント側アプリケーションプログラム部、802 クライアント側ファイルシステム部、803 クライアント側データ暗号/復号化実行部、901 代理サーバー、902 LAN、903、904 クライアント、1001 ファイルエントリ、1002 ユーザーIDフィールド、1003 ファイル名フィールド、1004 クライアント認証キーフィールド、1005 ファイルオープン属性フィールド、1006 ファイルのオープンアカウントフィールド、1007 先頭セクタの管理テーブルへのポインタフィールド、1008 ファイルのセクタ番号、1009 次管理テーブルへのポインタ、1010 セクタデータ領域へのポインタ、11 セクタデータ領域、3401 新暗号鍵、3601 ユーザーID、3602 旧暗号鍵、3603 新暗号鍵。

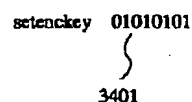
【図3】

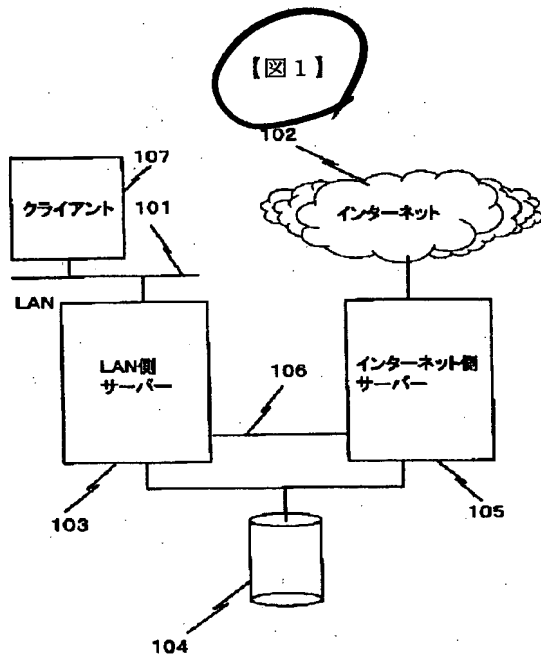


【図17】

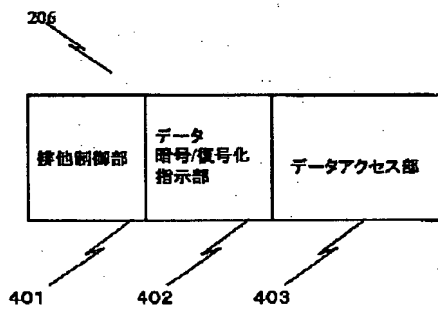


【図34】

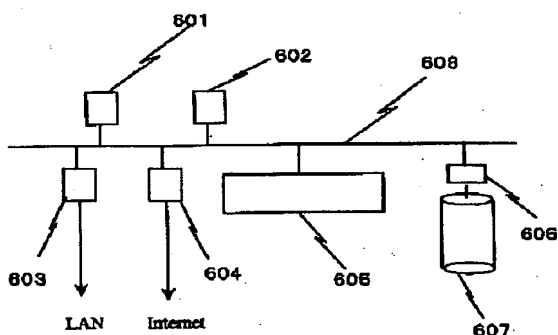




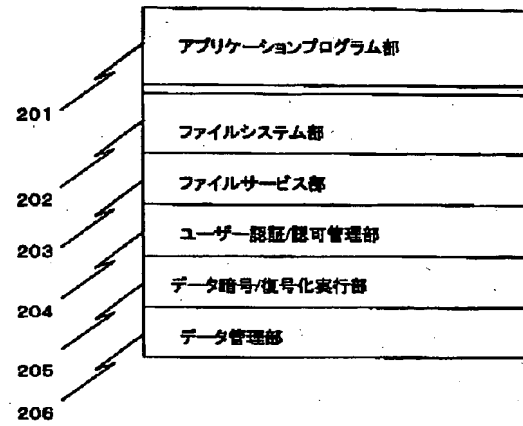
【図4】



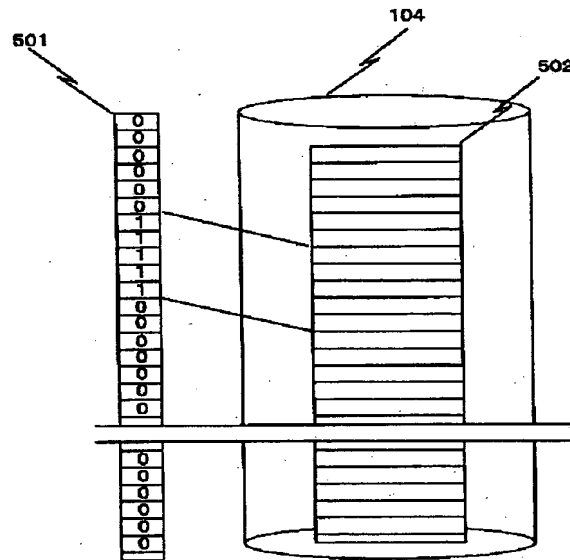
【図6】



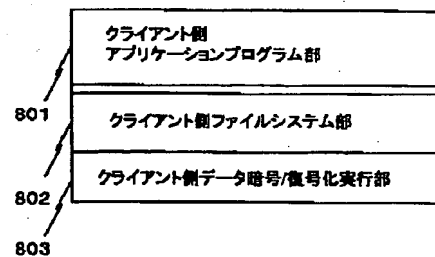
【図2】



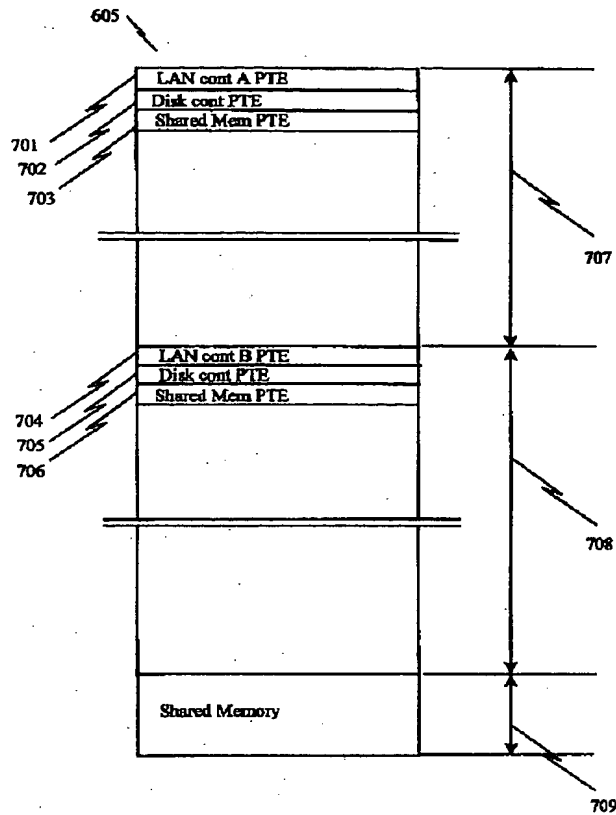
【図5】



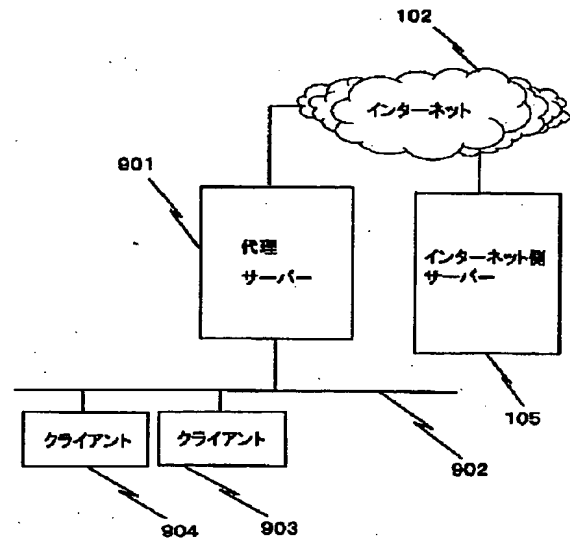
【図8】



【図7】



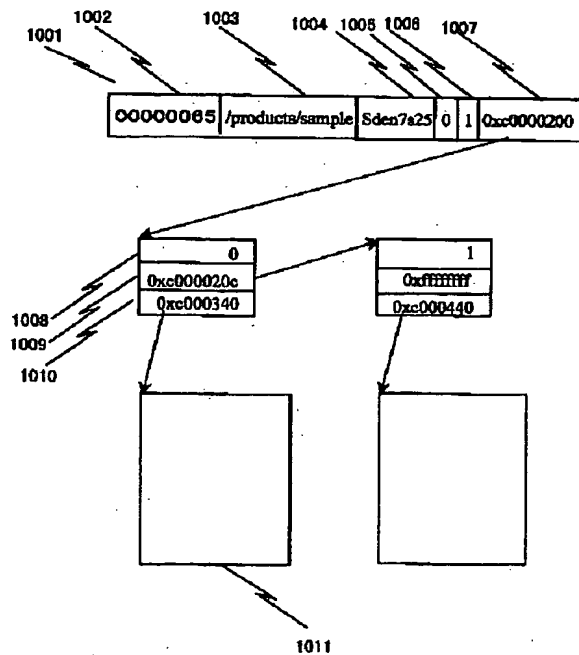
【図9】



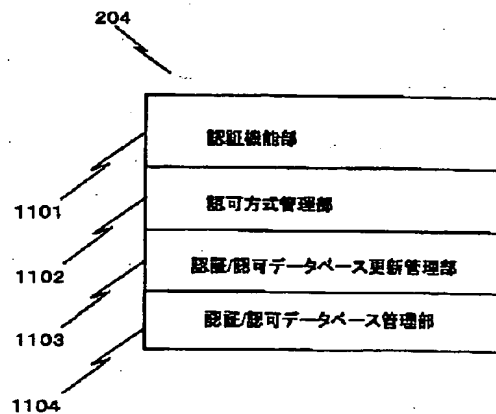
【図24】

00000000 00000065 Sden7s25 0 00000000 00000001 <データ例>
 2401 2402 2403 2404 2405 2406 2407

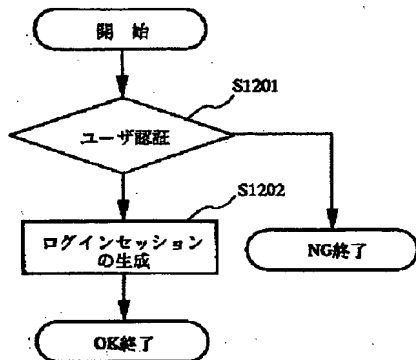
【図10】



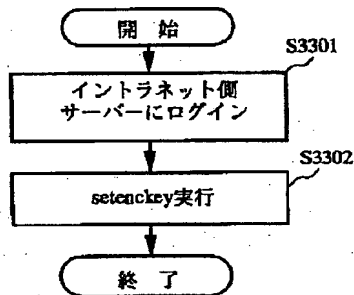
【図11】



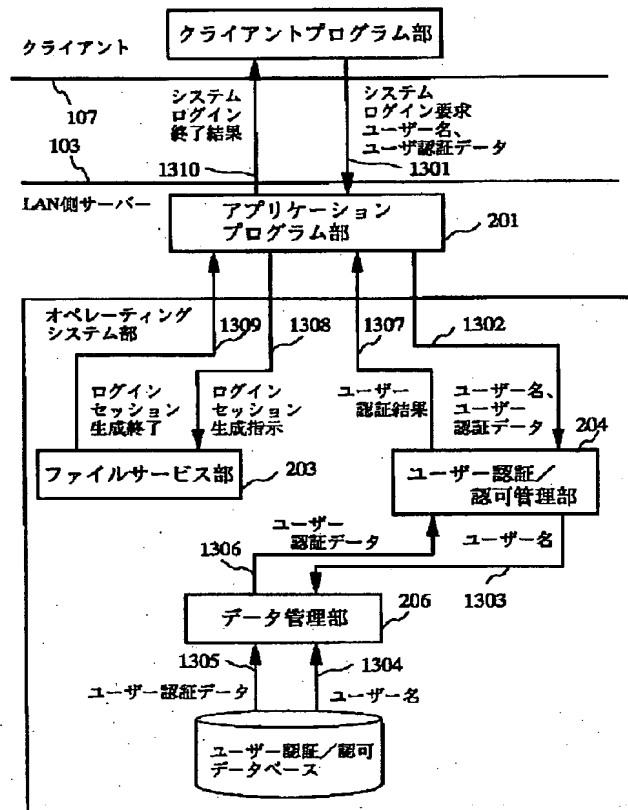
【図12】



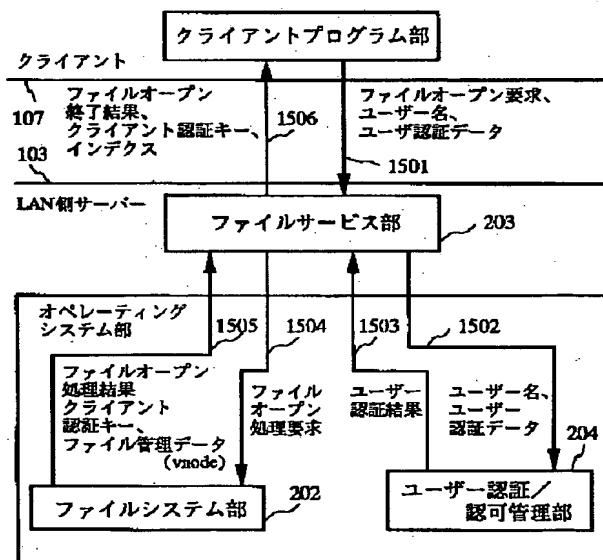
【図3.3】



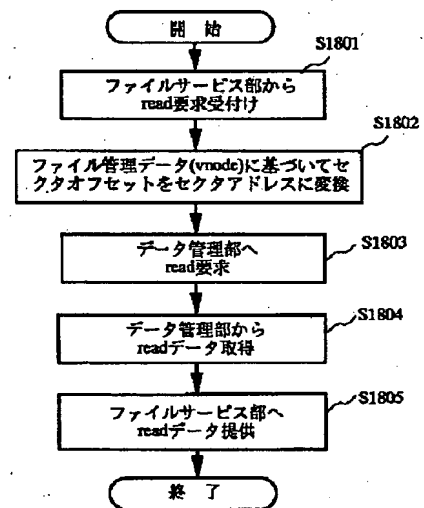
【図13】



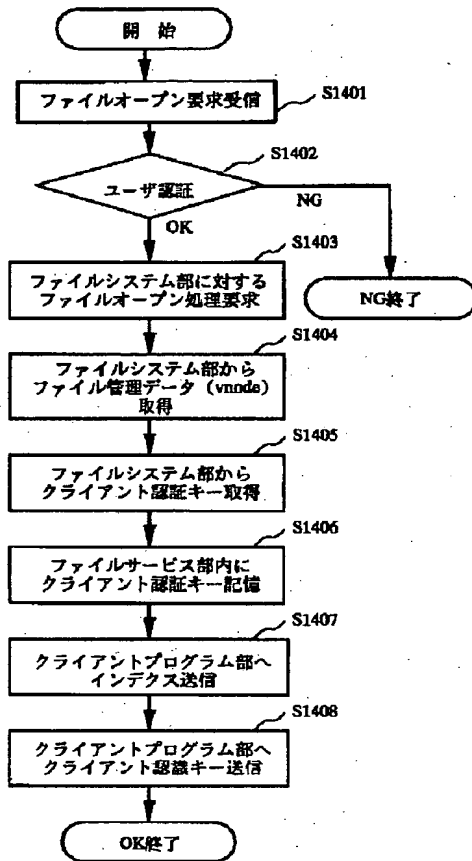
【図15】



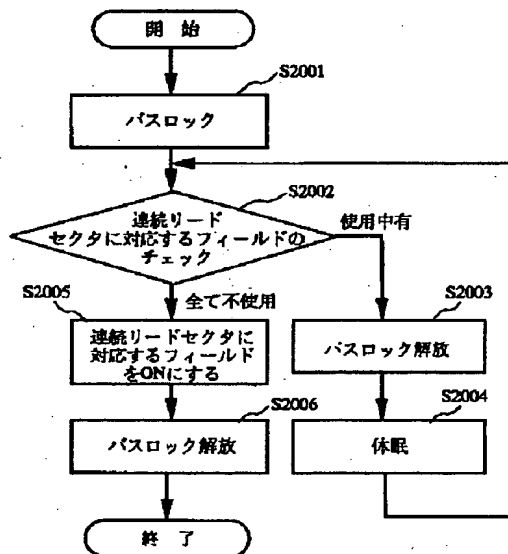
【図18】



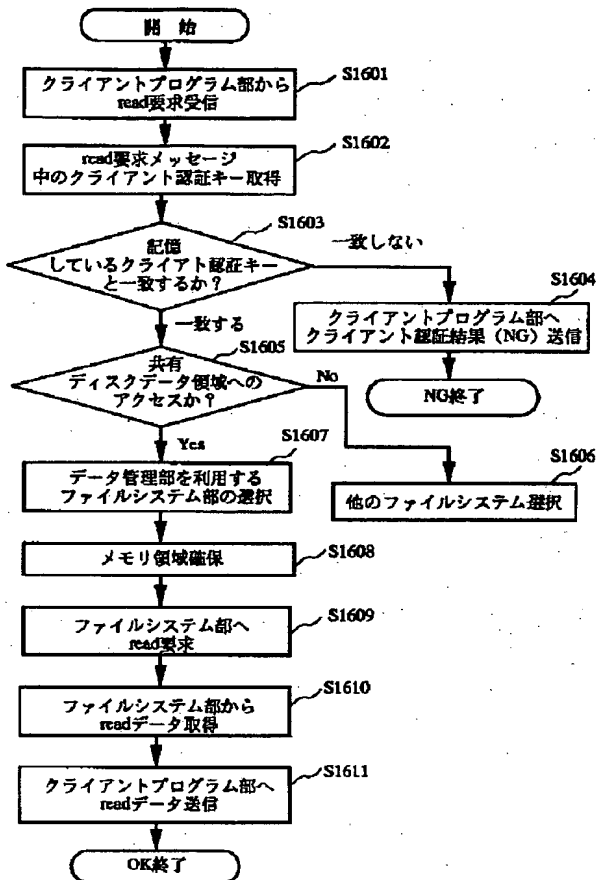
【図14】



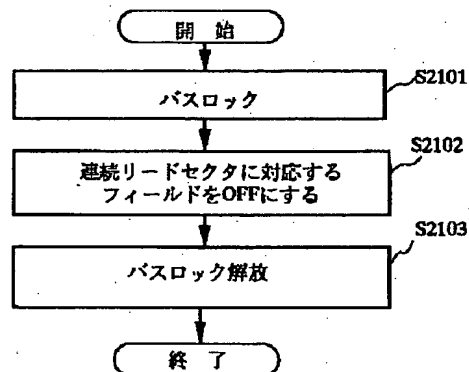
【図20】



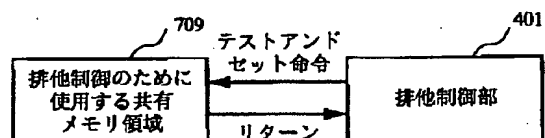
【図16】



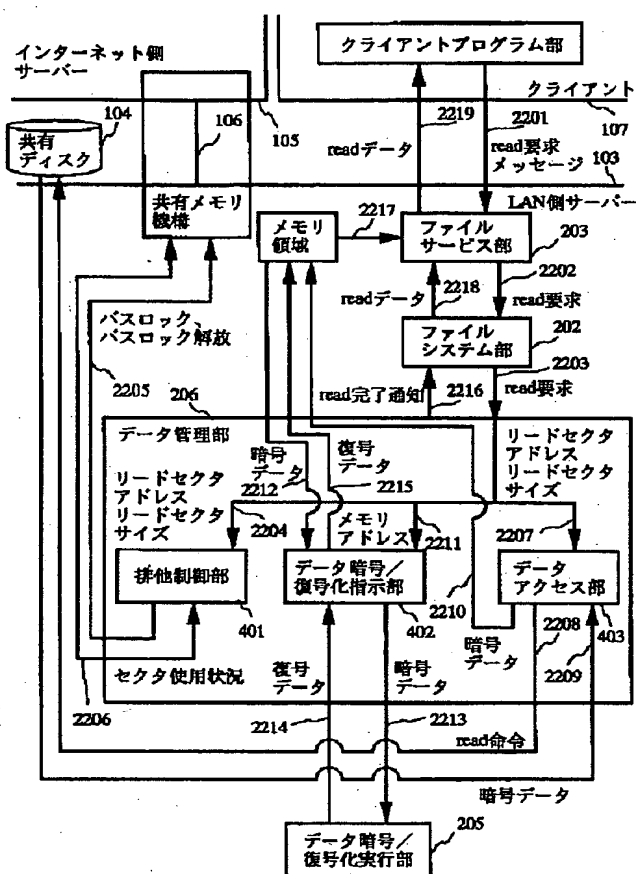
【図21】



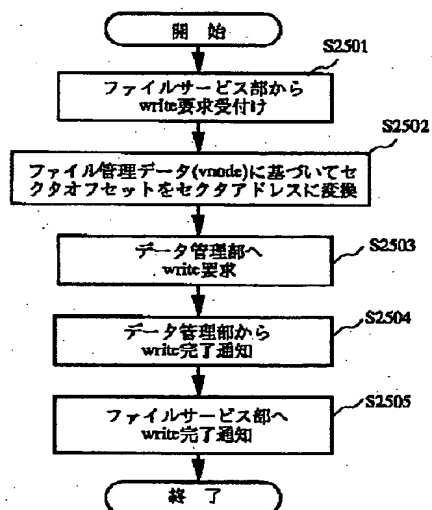
【図31】



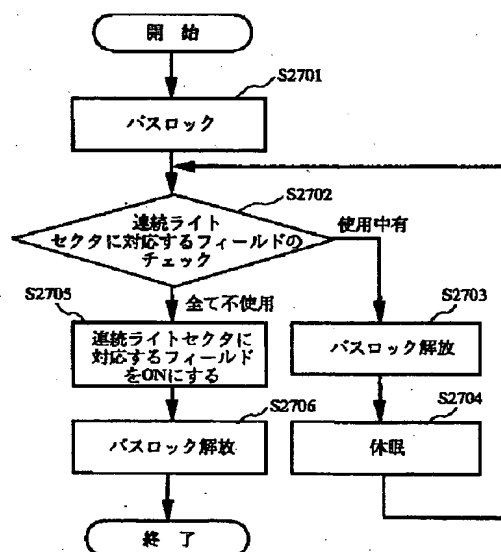
【图 2 2】



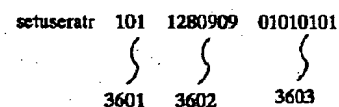
【图 2-5】



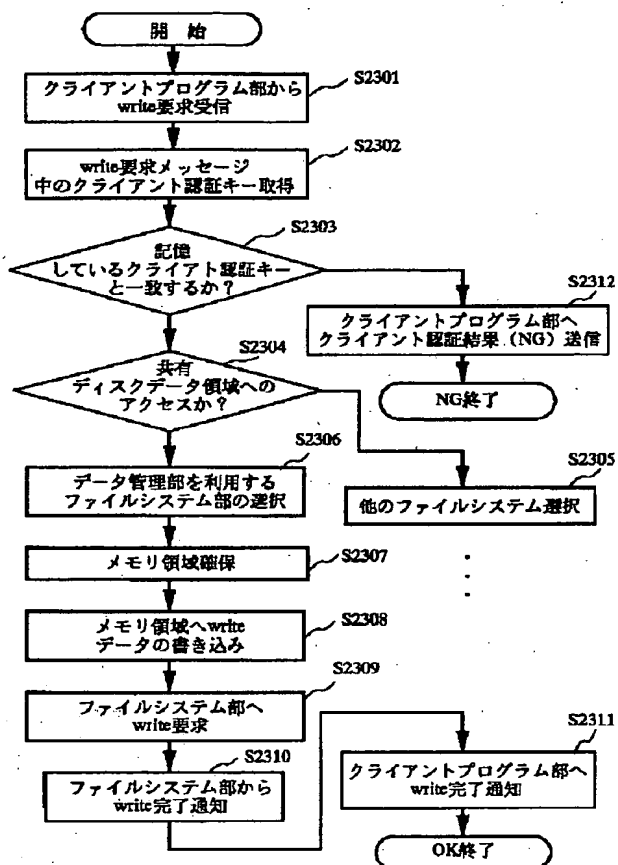
【图 27】



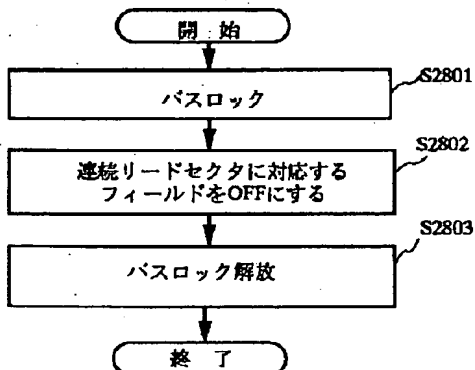
【图 3 6】



【図 23】



【図 28】

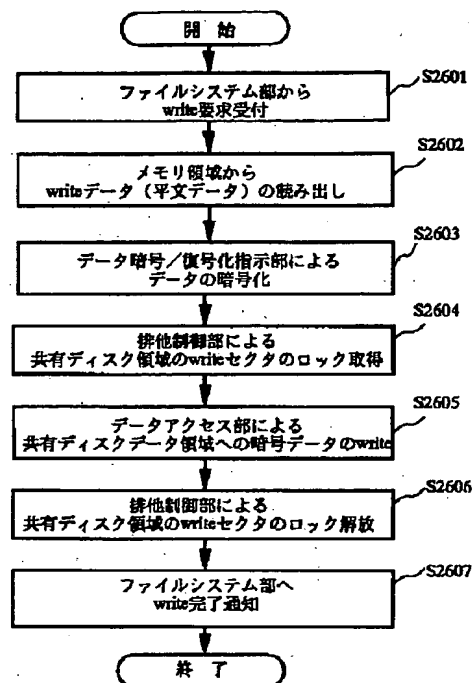


【図 48】

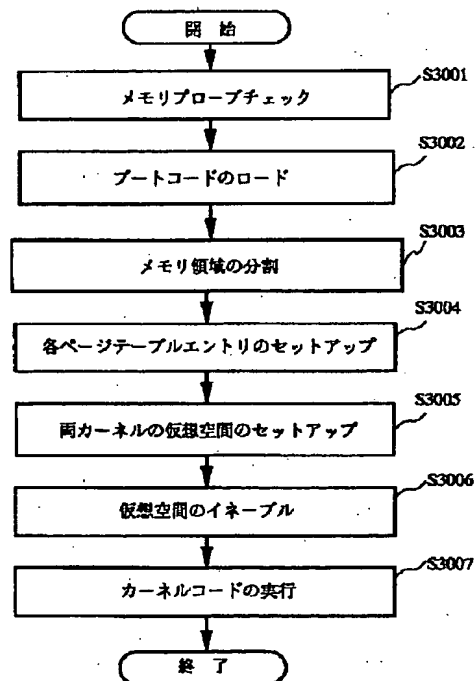
stale 00000065 /products/sample

4801 4802

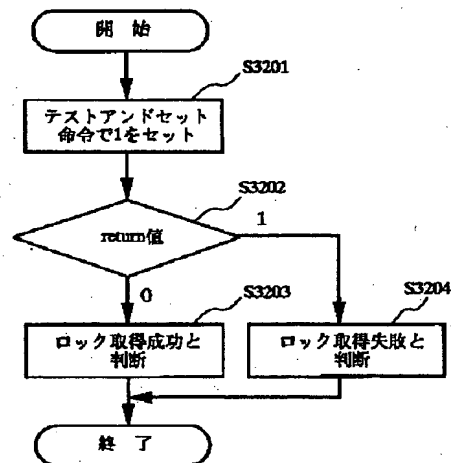
【図 26】



【図 30】



【図 3 2】

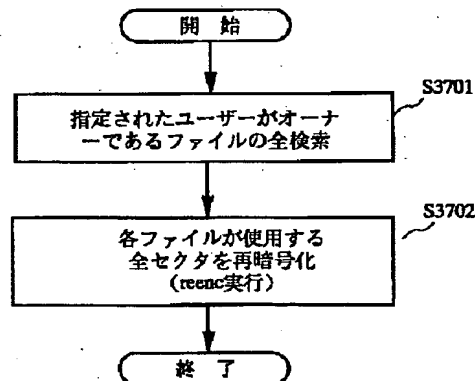


```

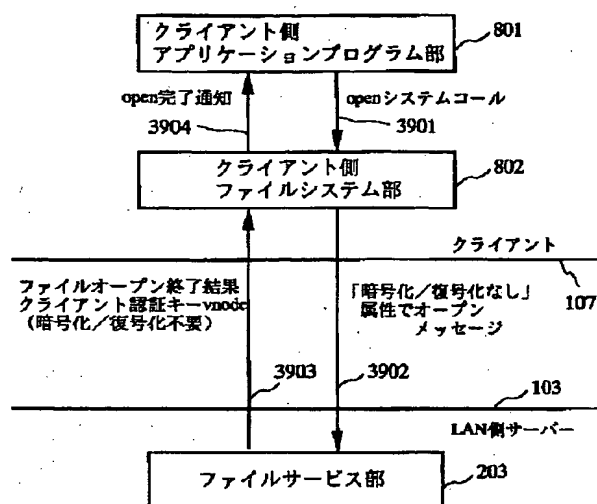
graph TD
    Start([開始]) --> S4901[非共有ディスク領域に  
新たなセクタ領域を確保]
    S4901 --> S4902[共有ディスク領域から  
セクタデータの読み出し]
    S4902 --> S4903[新たなセクタ領域へ  
セクタデータの書き込み]
    S4903 --> S4904[vnodeの更新]
    S4904 --> End([終了])
  
```

The flowchart illustrates the process for ensuring a new sector area in a non-shared disk area. It begins with a start node (開始), followed by step S4901: ensuring a new sector area in the non-shared disk area. This is followed by step S4902: reading out sector data from the shared disk area. Then, step S4903: writing the sector data to the new sector area. This is followed by step S4904: updating the vnode. The process ends at a terminal node (終了).

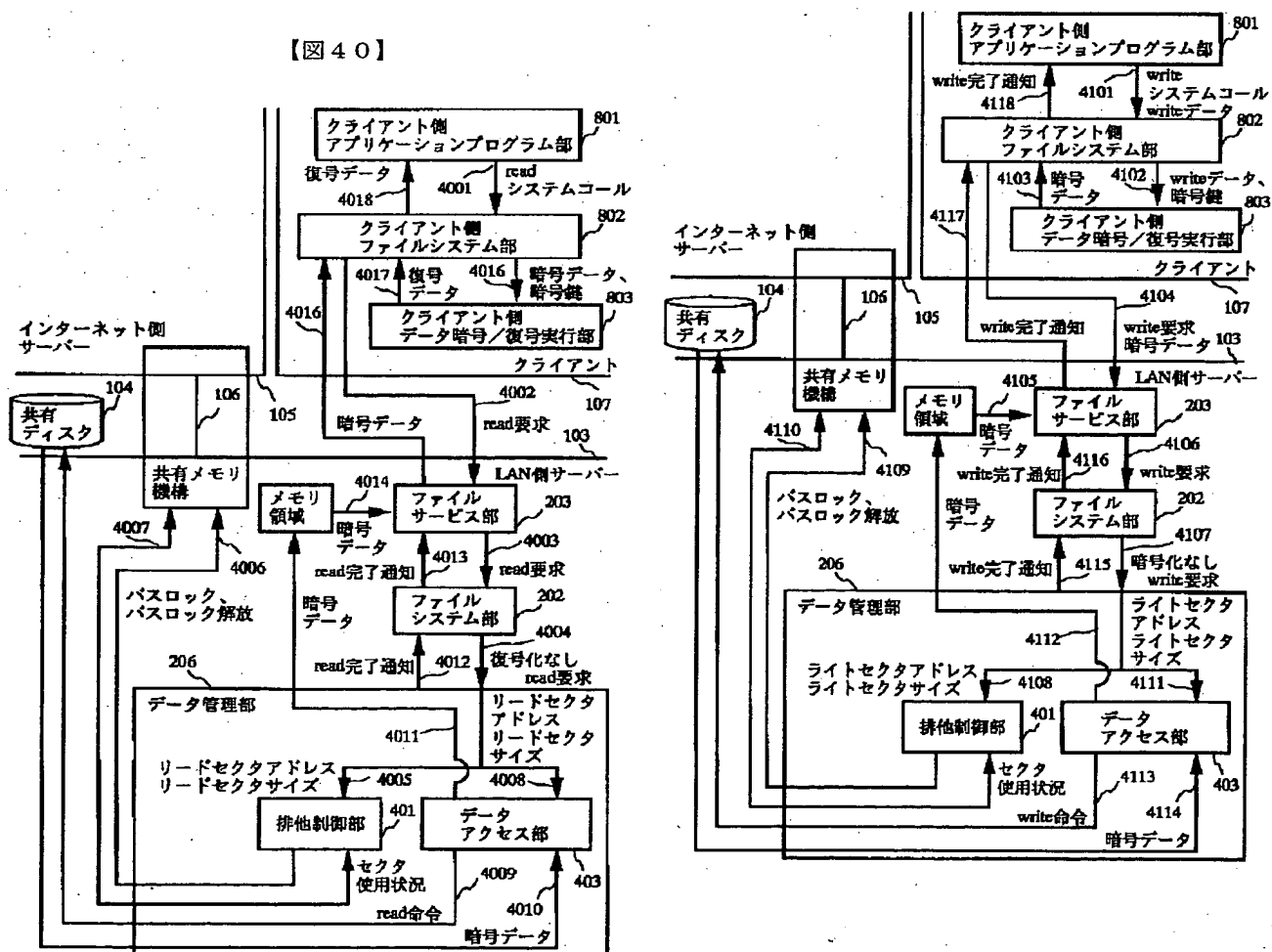
【図 3 7】



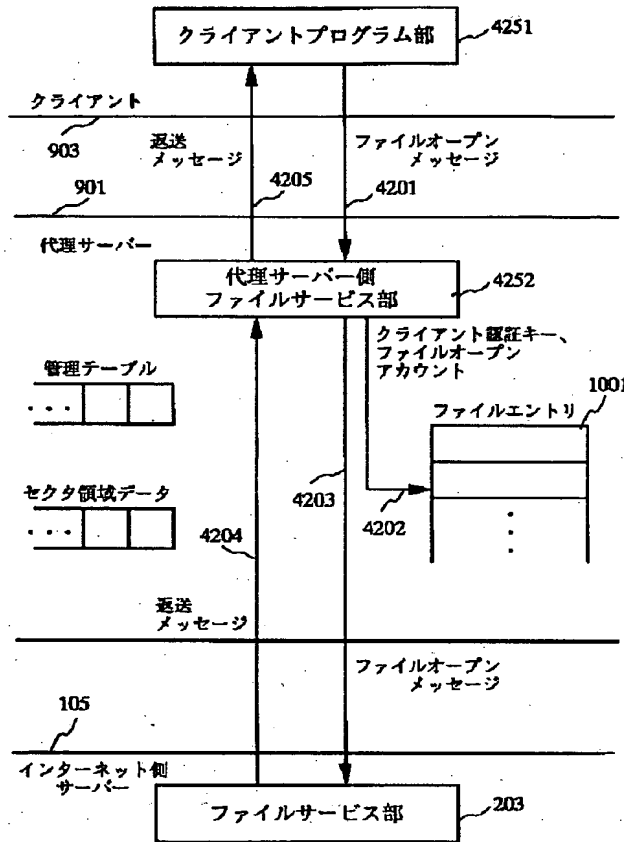
【图 39】



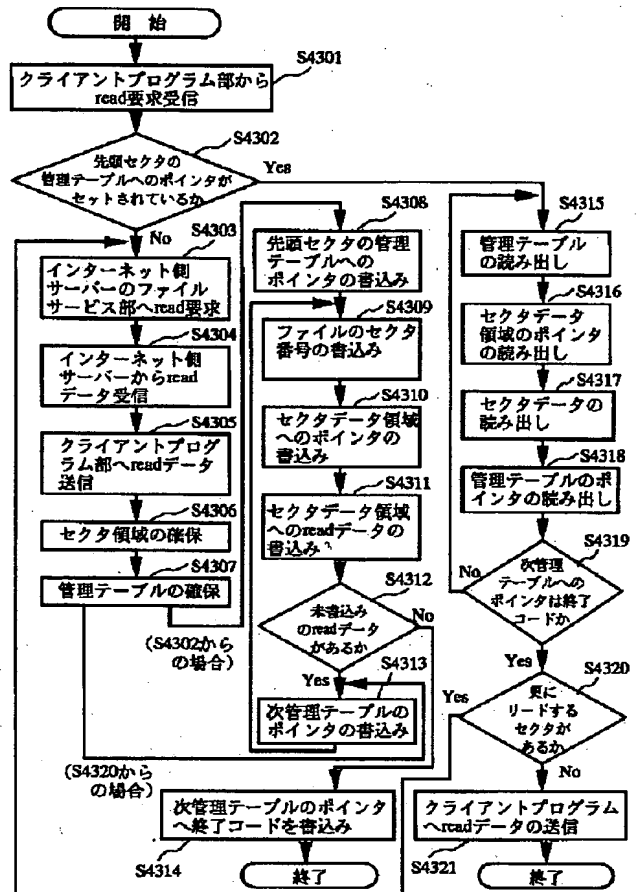
【图 4 1】



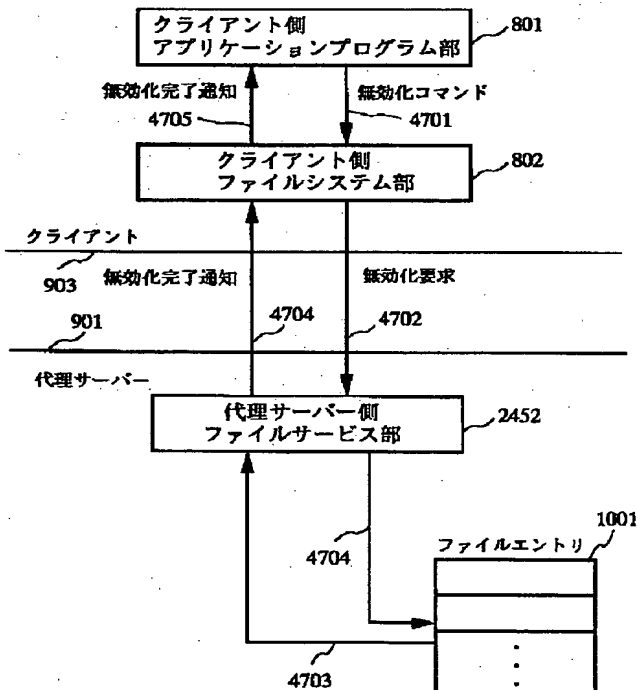
【図42】



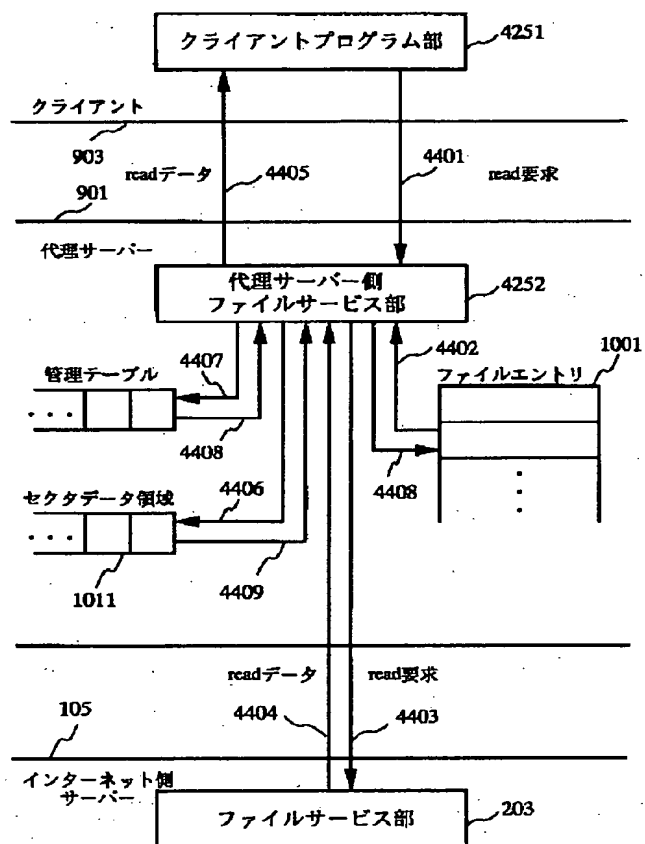
【図43】



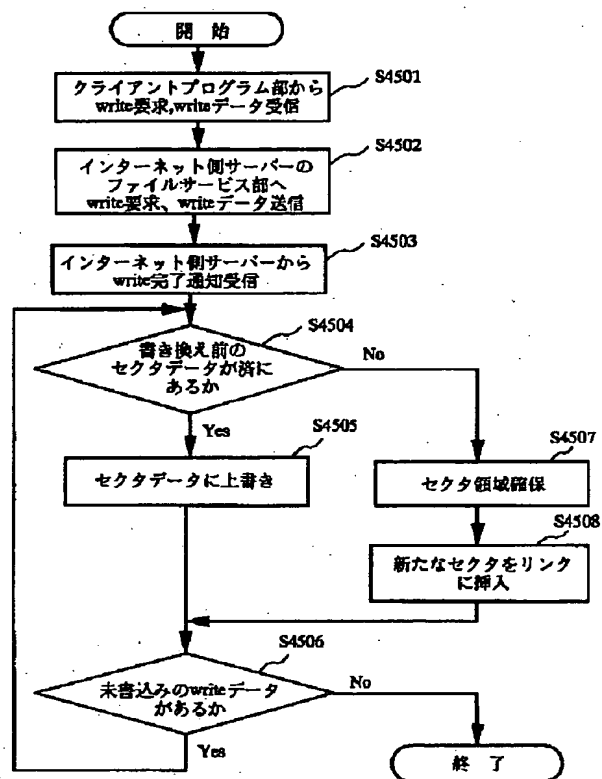
【図47】



【図 44】



【図 45】



【図46】

